

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局



(43) 国際公開日
2004 年 6 月 24 日 (24.06.2004)

PCT

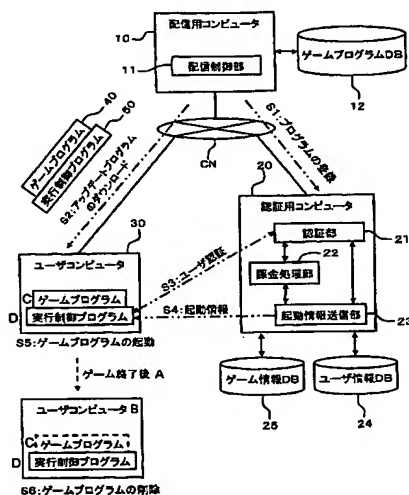
(10) 国際公開番号
WO 2004/053666 A1

- (51) 国際特許分類⁷: G06F 1/00 (72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 佐藤 健次 (SATO, Kenji) [JP/JP]; 〒141-0021 東京都品川区上大崎3丁目10番59号パレロワイヤル目黒101号 Tokyo (JP).
- (21) 国際出願番号: PCT/JP2003/015779
- (22) 国際出願日: 2003 年 12 月 10 日 (10.12.2003)
- (25) 国際出願の言語: 日本語 (74) 代理人: 上村 輝之, 外 (KAMIMURA, Teruyuki et al.); 〒101-0035 東京都千代田区神田紺屋町16クニビル2F Tokyo (JP).
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願 2002-359597
2002 年 12 月 11 日 (11.12.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): インターレックス株式会社 (INTERLEX INC.) [JP/JP]; 〒108-0023 東京都港区芝浦2丁目17番13号 Tokyo (JP).
- (81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

[続葉有]

(54) Title: SOFTWARE EXECUTION CONTROL SYSTEM AND SOFTWARE EXECUTION CONTROL PROGRAM

(54) 発明の名称: ソフトウェア実行制御システム及びソフトウェアの実行制御プログラム



- 10...DISTRIBUTION COMPUTER
11...DISTRIBUTION CONTROL SECTION
12...GAME PROGRAM DB
40...GAME PROGRAM
50...EXECUTION CONTROL PROGRAM
S2...DOWNLOAD UPDATE PROGRAM
S1...REGISTER PROGRAM
30...USER COMPUTER
S3...USER AUTHENTICATION
S4...START INFORMATION
S5...GAME PROGRAM START
20...AUTHENTICATION COMPUTER
21...AUTHENTICATION SECTION
22...ACCOUNTING SECTION
23...START INFORMATION TRANSMISSION SECTION
A...AFTER GAME END
B...USER COMPUTER
C...GAME PROGRAM
D...EXECUTION CONTROL PROGRAM
S6...GAME PROGRAM DELETION
25...GAME INFORMATION DB
24...USER INFORMATION DB

(57) Abstract: It is possible to prevent unauthorized use of software such as a game program in download type software distribution for using a program and data by storing them in a user computer in advance. A user downloads (S2) a game program (40) of new version (including an accompanying data group) and an execution program (50) from a distribution computer (10). The execution control program (50) performs authentication by online with an authentication computer (20) and acquires (S3, S4) start information required for starting the game program (40). The execution control program (50) decodes the game program (40) according to the start information and starts it (S5). When the user terminates the game by terminating the game program (40), the execution control program (50) deletes all or a part of the game program (40) so as to incapacitate it (S6).

(57) 要約: 【課題】ユーザコンピュータに予めプログラムやデータを格納させて利用するダウンロード式のソフトウェア配信において、ゲームプログラム等のソフトウェアの違法な使用を未然に阻止する。【解決部】ユーザは、配信用コンピュータ10から新版のゲームプログラム40(付随データ群も含む)及び実行制御プログラム50をダウンロードする(S2)。実行制御プログラム50は、認証用コンピュータ20とオンラインによる認証を行って、ゲームプログラム40を起動させるために必要な起動情報を取得する(S3,S4)。実行制御プログラム50は、起動情報に基づいてゲームプログラム40をデコードし、起動させる(S5)。ユーザがゲームを終えて、ゲームプログラム40を終了させると、実行制御プログラム50は、ゲームプログラム40の全部又は一部を削除することにより無力化する(S6)。



(84) 指定国 (広域): ARIPO 特許 (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告書

2 文字コード及び他の略語については、定期発行される各 *PCT* ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明 細 書

ソフトウェア実行制御システム及びソフトウェアの実行制御プログラム

5

技 術 分 野

本発明は、例えば、ゲームソフトウェア、文書や図形等を作成する実務用ソフトウェア等の各種アプリケーションソフトウェアを新バージョンのソフトウェアに更新させたり、その実行を制御するソフトウェア実行制御システム及びソフトウェアの実行制御プログラムに関する。

10

技 術 背 景

一般的に、例えば、パーソナルコンピュータや携帯情報端末等のユーザコンピュータ上で稼働するゲームソフトウェア等のアプリケーションソフトウェアは、
15 例えば、OS (Operating System)、使用言語、ハードウェア構成等の各種のソフトウェア実行環境に応じて、あるいは、ソフトウェアの価格や代金支払いの有無等に応じて、複数種類のバージョンが用意されることがある。

例えば、同じソフトウェアであっても、英語版、日本語版、中国語版等のように、使用言語毎に異なるバージョンが用意されることがある。また、無償で提供するバージョンと有償で提供するバージョンとを用意し、無償のソフトウェアから有償のソフトウェアへバージョンアップを誘導することも比較的よく行われている。無償のソフトウェアは、「体験版」や「お試し版」とも呼ばれ、有償のソフトウェアは「製品版」や「完全版」とも呼ばれる。無償のソフトウェアは、同種の有償のソフトウェアに比べて、その機能が一部制限されていたり、試用期間や
25 試用回数に制限を受けることが多い。無償のソフトウェアを試用することにより

ソフトウェアの価値を認めたユーザは、提供元のウェブサイトから有償のソフトウェアを購入してダウンロードしたり、販売店で有償のパッケージソフトウェアを購入したりしてバージョンアップを行う。

一方、ソフトウェアはデジタルデータであり、複製が容易で、かつ複製による劣化も殆ど生じないという特徴を有するため、違法コピーや無断使用が大きな問題となっている。そこで、ソフトウェア（ソフトウェアのライセンス）を購入した正規ユーザとライセンスを得ていない違法ユーザとを、ユーザ認証等によって識別し、正規ユーザにのみソフトウェアを使用させるようにすることが従来より行われている。

- 10 例えば、ソフトウェアをインストールする際に、ソフトウェアパッケージや記録媒体に印刷されたプロダクトIDを入力させて、正規購入品であるか否かを判定する技術は知られている（例えば、特開2002-258963号公報 段落0003参照）。

また、ソフトウェアを使用するための鍵データを、イントラネット上に設置されたライセンス管理サーバに要求し、ユーザ認証により正当なユーザと認められた場合には、ライセンス管理サーバから鍵データを取得し、この鍵データによってソフトウェアを起動させて使用するようにしたものも知られている（例えば、特開2002-6972号公報、特開2002-297254公報）。

プロダクトID（プロダクトキー）を入力することにより正規ユーザであるか否かを判別する従来技術は、単なる文字や記号からなるIDをインストール時に
20 入力するだけの防御機構であり、容易に回避可能である。従って、この種の防御機構（著作権保護機構）しか備えないソフトウェアは、違法コピーや無断使用を事実上排除することができない。

ライセンス管理サーバとの間でユーザ認証を行い、正常に認証された場合に鍵
25 データをユーザコンピュータに送信して起動させる技術は、単にプロダクトID

を入力するだけの技術に比べて、防御力は向上している。しかし、ソフトウェアはユーザコンピュータ上で既に起動可能状態に置かれており、鍵データの取得待ちとなっている。従って、鍵データの入力待ち状態となっているソフトウェアを違法コピーし、別の方法で鍵データを取得してしまえば、防御機構をすり抜けて

5 使用することができる。

一方、近年では、コンピュータの処理能力増大及び通信ネットワークの高速化等に伴って、ユーザが希望する時に希望のソフトウェアを実行させる方法が提案されている。このようなソフトウェアのオンデマンド配信に適用可能な配信方法としては、ストリーミング方式とダウンロード方式とが知られている。

10 ストリーミング方式では、ユーザコンピュータは、サーバからソフトウェアを受信しながら同時に再生を行う。そして、再生を終了して不要になったデータは直ちに破棄される。従って、ストリーミング方式は、ユーザの閲覧が終了した時点でデータが残らないため、特殊なソフトウェアを用いる等しない限り、違法にソフトウェアをコピーすることができない。しかし、ストリーミング方式では、

15 ユーザが視聴を希望するたび毎に毎回ソフトウェアのデータを送信する必要があるため、広帯域で高速な通信ネットワークが整備されている場合でも、多数のユーザが同時にストリーミング配信を希望すると、通信ネットワークのトラフィックが増大し、サーバの負担も大きくなる。

これに対し、ダウンロード方式の場合は、ユーザの希望するソフトウェアをサーバからユーザコンピュータにダウンロードさせて蓄積し、ユーザコンピュータ
20 上で実行させるため、データが通信ネットワークを流れる時間は少なく、多数のユーザからの配信要求に応えることができる。しかし、ダウンロード方式の場合は、ユーザコンピュータ内にソフトウェアが蓄積されたままになるため、ストリーミング方式よりも簡単に違法コピー等を行うことができる。

25 また、例えば、CD - ROM、DVD - ROM、ハードディスク、半導体メモリ等

の各種記録媒体にゲームプログラム等を固定して流通に置くことも広く行われている。この場合も、上述の通り、ゲームプログラム等が不正にコピーされたり、プロテクト機構が不正に破られたりして、不正に使用されている。

5

発 明 の 開 示

そこで、本発明の1つの目的は、ソフトウェアの不正使用を抑制できるようにしたソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

- 10 本発明の1つの目的は、ユーザコンピュータにソフトウェアを保存して実行させるダウンロード方式の場合に、違法コピーや無断使用を防止できるようにしたソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

- 15 本発明の1つの目的は、ソフトウェアの実行中に不正な使用が行われるのを未然に防止できるようにしたソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

本発明の1つの目的は、負荷状態等を考慮しながら、不正使用に対する監視効率を動的に制御することができるソフトウェア実行制御システム及びソフトウェアの実行制御プログラムを提供することにある。

- 20 本発明の他の目的は、後述する実施の形態の説明から明らかになるであろう。

本発明に係るソフトウェア実行制御システムは、ユーザコンピュータにインストールされた第1のソフトウェアを第2のソフトウェアに更新させるものであって、後述の配信部及び認証部を備え、かつ、特徴的な動作を行う実行制御プログラムを採用する。

- 25 配信部は、エンコードされた第2のソフトウェア及び該第2のソフトウェアの

実行を制御するための実行制御プログラムをユーザコンピュータに通信ネットワークを介して配信するものである。認証部は、ユーザコンピュータにインストールされた実行制御プログラムからの要求によってユーザ認証を行い、正当なユーザであると確認した場合には、第2のソフトウェアをデコードして起動させるために必要な所定の情報を通信ネットワークを介して実行制御プログラムに送信するものである。そして、第2のソフトウェアは実行制御プログラムから渡される起動情報のみで起動可能に構成されており、実行制御プログラムは、(1) 認証部から受信した所定の情報に基づいてエンコードされた第2のソフトウェアをデコードして第1のソフトウェアに置き換え、(2) 所定の情報に基づいて起動情報を生成することにより、第2のソフトウェアを起動させ、(3) 第2のソフトウェアの実行が終了された場合には、第2のソフトウェアを無力化させるように構成されている。

第1のソフトウェアと第2のソフトウェアとは、同一種類のソフトウェアであって、バージョンの異なるものである。第1のソフトウェアを旧版ソフトウェア、第2のソフトウェアを新版ソフトウェアと呼ぶこともできる。第1、第2のソフトウェアとしては、例えば、ゲーム、映画、娯楽番組、教養番組、教育番組、文書作成、図形作成、画像編集等の各種アプリケーションソフトウェアを採用することができる。第1のソフトウェアと第2のソフトウェアとは、例えば、使用言語、実行可能環境(対応OS等)、機能制限の有無等で相違する。ユーザコンピュータとしては、例えば、ワークステーション、パーソナルコンピュータ、携帯情報端末、携帯電話等を挙げることができる。

最初に、ユーザコンピュータにインストールされている第1のソフトウェアは、後述の認証処理等を行わずに、ユーザが自由に使用することができる。第1のソフトウェアは、例えば、ソフトウェアベンダーのサイトからインターネット等の通信ネットワークを介して、あるいは、店頭販売のパッケージソフトウェアによ

って、ユーザコンピュータにインストールされている。

次に、ユーザが、配信部から第2のソフトウェアのダウンロードを希望すると、第2のソフトウェア及び第2のソフトウェアの実行を制御する実行制御プログラムが配信部からユーザコンピュータに送信される。実行制御プログラムは、ユーザコンピュータ上で実行される。実行制御プログラムは、通信ネットワークを介して認証部にユーザ認証を要求する。ユーザ認証の方法としては、例えば、ユーザID、パスワード、ユーザコンピュータに固有の情報（例えば、MACアドレス（Media Access Control address）等）を予め登録されているデータと照合することにより行うことができる。なお、これに限らず、例えば、指紋や声紋等のユーザ固有の生体情報を用いて認証を行うようにしてもよい。

認証部が正当なユーザであると認証した場合は、認証部からユーザコンピュータの実行制御プログラムに向けて、所定の情報が送信される。この所定の情報には、エンコードされた状態でユーザコンピュータに送信された第2のソフトウェアをデコードし、デコードされた第2のソフトウェアを起動させるために必要なデータが含まれている。

ここで、第2のソフトウェアは、実行制御プログラムから渡される起動情報のみで起動可能に構成されている。即ち、実行制御プログラムは、第2のソフトウェアを起動させる専用の「ランチャーソフトウェア」として作用する。

そして、実行制御プログラムは、以下の処理を行う。（1）まず、実行制御プログラムは、認証部から受信した所定の情報に基づいて（所定の情報に含まれるデコードキーを利用して）、第2のソフトウェアをデコードする。デコードされた第2のソフトウェアは、第1のソフトウェアに置き換えられる。（2）次に、実行制御プログラムは、認証部から受信した所定の情報に基づいて（所定の情報に含まれる起動引数を利用して）、起動情報（起動引数とデコードされた第2のソフトウェアのレジストリパスからなる起動ステートメント）を生成し、この起動情報に

よって第2のソフトウェアを起動させる。これにより、ユーザは、ユーザコンピュータ上で第2のソフトウェアを使用することができる。(3) 実行制御プログラムは、第2のソフトウェアの起動後も、第2のソフトウェアの実行状態を監視しており、第2のソフトウェアの実行終了を検出すると、第2のソフトウェアを無
5 力化させる。これにより、ユーザは、第2のソフトウェアを使用することができなくなる。

ユーザが再度の使用を希望する場合、再び認証部による認証を受けて所定の情報を取得すればよい。あるいは、再びユーザコンピュータを配信部にアクセスさせて、第2のソフトウェアを再度ダウンロードしてもよい。第2のソフトウェア
10 の全体を再度ダウンロードする必要はなく、プログラム部分のみを再ダウンロードするように構成すれば、通信時間を短縮し、トラフィックを低減させることができる。なお、認証部からユーザコンピュータに向けて送信される所定の情報は、暗号化されているのが好ましい。

第2のソフトウェアの実行が終了すると、実行制御プログラムは、第2のソフトウェアを無力化させる。無力化とは、第2のソフトウェアを起動したり、実行
15 したりできなくすることを意味する。無力化の方法としては、種々のものを採用することができる。例えば、デコードされた第2のソフトウェアの全体を削除することにより無力化することができる。また、デコードされた第2のソフトウェアの一部を削除することによっても無力化することができる。なお、一部のみを
20 削除する場合は、その削除した部分及び起動引数を認証部から受信することにより、第2のソフトウェアを再起動させることができる。あるいは、第2のソフトウェアがプログラムと付随データ群とを含んでなる場合、プログラムのみを削除することでも第2のソフトウェアを無力化させることができる。なお、デコード
25 前のエンコードデータを保存しておくことにより、認証部から所定の情報を再度受信するだけで第2のソフトウェアを再び使用することができる。付随データ群

とは、プログラムの実行に際して利用されるプログラム以外のデータ群を意味し、例えば、画像データ、音声データ、楽曲データ、テキストデータ等を挙げることができる。

好適な実施形態では、実行制御プログラムは、複数種類の第2のソフトウェア
5 に対応可能に構成されており、認証部が実行制御プログラムに送信する所定の情報には、起動させる第2のソフトウェアの格納先アドレス情報と起動引数と第2のソフトウェアをデコードするためのデコードキー情報とが含まれる。

通信ネットワークを介したリアルタイムのオンライン認証と第2のソフトウェアの起動及び終了を制御する実行制御プログラムは、第2のソフトウェアとは別
10 体に生成されている。従って、1種類の実行制御プログラムを用意するだけで、多種類の第2のソフトウェアに対応することができる。

好適な実施形態では、実行制御プログラムは、ユーザコンピュータに固有のマシン情報と暗号化キー情報とを含む認証用情報を認証部に送信し、認証部は、少なくともマシン情報に基づいてユーザ認証を行い、正当なユーザであると確認し
15 た場合には、所定の情報を暗号化キー情報で暗号化して通信ネットワークを介して実行制御プログラムに送信するものであり、かつ、認証部には、マシン情報を複数個登録可能に構成されている。

ユーザコンピュータに固有のマシン情報としては、例えば、MAC アドレス等を挙げることができる。これに加えて、ユーザコンピュータの構成情報（例えば、
20 搭載メモリ量、CPUスペック、サウンドチップやグラフィックアクセラレータの製品名等）を採用してもよい。認証部には、複数個のマシン情報を登録させることができる。これにより、第2のソフトウェアのライセンスを正当に購入したユーザは、例えば、自宅のパーソナルコンピュータと職場のパーソナルコンピュータ等のように、複数台のユーザコンピュータを用いて、同一の第2のソフトウ
25 エアを利用することができる。

好適な実施形態では、認証部は、正当なユーザであると確認した場合には、該ユーザが起動可能な第2のソフトウェアの一覧データをユーザコンピュータに送信し、一覧データから選択された第2のソフトウェアに関する所定の情報を通信ネットワークを介して実行制御プログラムに送信する。

- 5 ユーザが複数種類の第2のソフトウェアのライセンスを正式に購入済の場合もあるが、認証部は、ユーザ認証後に、そのユーザが利用可能な第2のソフトウェアの名称等を列挙した一覧データをユーザコンピュータに送信する。ユーザは、起動可能な（利用可能な）一覧メニューから起動を望む第2のソフトウェアを選択する。これにより、認証部は、選択された第2のソフトウェアをデコードし起
10 動するための所定の情報を生成し、実行制御プログラムに送信する。

- 好適な実施形態では、実行制御プログラムは、ユーザコンピュータに固有のマシン情報を取得する機能と、暗号化キー情報を生成する機能と、認証部にユーザ認証を要求し、少なくともマシン情報及び暗号化キー情報を認証部に送信する機能と、認証部から受信した起動可能な第2のソフトウェアの一覧データからい
15 ずれか1つの第2のソフトウェアをユーザに選択させ、選択された第2のソフトウェアを認証部に通知する機能と、選択された第2のソフトウェアのユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを少なくとも暗号化キー情報により暗号化してなる所定の情報を受信する機能と、暗号化された所定の情報を少なくとも暗号化キー情報により解読する機能と、解読された
20 デコードキー情報によりユーザコンピュータ内の第2のソフトウェアをデコードさせる機能と、解読された起動引数及び格納先アドレス情報に基づいて、起動情報を生成する機能と、生成された起動情報によってデコードされた第2のソフトウェアを起動させる機能と、起動された第2のソフトウェアの実行状態を監視し、該第2のソフトウェアの実行が終了した場合は、第2のソフトウェアを無力化さ
25 せる機能と、をユーザコンピュータ上に実現させる。

また、好適な実施形態では、第2のソフトウェアは、プログラムと付随データ群とを含んでなり、プログラム又は付随データ群の少なくともいずれか一方を更新させるようになっている。

ここで、ユーザコンピュータにインストールされている第1のソフトウェアは、
5 第2のソフトウェアに置換されるまでは、認証部による認証を受けることなく実行可能である。

また、好適な実施形態では、実行制御プログラムは、第2のソフトウェアとは別に強制終了させることができないプログラムとして構成されている。

即ち、例えば、稼働中のタスクを管理するプログラム等を用いて、実行制御プログラムのみを強制終了させることができないように構成されている。実行制御プログラムによる監視を停止させて、第2のソフトウェアのみをコピー等できないようにするためである。より具体的には、ハードウェアを指定しないデバイスドライバとして実行制御プログラムを生成すれば（ハードウェアを指定しないので、厳密にはデバイスドライバではないが）、アプリケーションプログラムよりも
15 OS側に近いプログラムあるいはOSの一部を構成するプログラムとして構成されるため、通常のアプリケーションプログラムのように強制的に終了させることが困難となる。強制終了させにくいプログラムとしては、ドライバプログラムの他にBIOS（Basic Input/Output System）も知られている。しかし、BIOSは、基本的に、ハードウェアとの間で直接データを送受信するだけの機能しか持たない
20 ため、暗号化されたデータを復号化したり、第2のソフトウェアの実行を監視したりする等の高度な制御を行うことができない。このように、実行制御プログラムを、例えば、デバイスドライバのように、OSとアプリケーションプログラム（第2のソフトウェア）との間に位置する中間プログラムとして構成することにより、高度な処理を行わせつつ、悪用を防止することができる。

25 好適な実施形態では、配信部と認証部とは、それぞれ別体のコンピュータ上に

実現されている。

例えば、第2のソフトウェア及び実行制御プログラムを配信する配信部は、各ソフトウェア会社毎にそれぞれ設置し、第2のソフトウェアの起動時認証を行う認証部は、各国、各地域、各ソフトウェア会社の団体毎に設置することができる。

5 本発明は、プログラムの発明としても把握することができる。

即ち、ユーザコンピュータにインストールされた第1のソフトウェアを第2のソフトウェアに更新し、この第2のソフトウェアの実行を制御する実行制御プログラムであって、外部の認証部と通信ネットワークを介して通信し、ユーザ認証を求める第1の機能と、認証部から受信した所定の情報に基づいて、第2のソフトウェアを起動させるための起動情報を生成する第2の機能と、認証部から受信した所定の情報に基づいて、第2のソフトウェアをデコードさせる第3の機能と、ユーザコンピュータに既にインストールされている更新前のソフトウェアをデコードされた第2のソフトウェアに置き換える第4の機能と、生成された起動情報によって第2のソフトウェアを起動させる第5の機能と、第2のソフトウェアの
10 実行状態を監視し、第2のソフトウェアの実行が終了した場合は、第2のソフトウェアを無力化させる第6の機能と、をユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

また、本発明は、ソフトウェアの更新方法としても把握できる。

即ち、ユーザコンピュータにインストールされている自由に使用可能な第1のソフトウェアを第2のソフトウェアに更新可能である旨をユーザに通知させるステップと、第2のソフトウェアを配信する配信用コンピュータにユーザコンピュータを通信ネットワークを介して接続させ、第2のソフトウェアへの更新を要求させるステップと、配信用コンピュータからユーザコンピュータにエンコードされた第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行
20 制御プログラムを通信ネットワークを介して送信させるステップと、ユーザコン

コンピュータ上で起動した実行制御プログラムにより、ユーザコンピュータと認証用コンピュータとを通信ネットワークを介して接続させ、認証用コンピュータにユーザ認証を要求させるステップと、ユーザ認証により正当なユーザであると認められた場合に認証用コンピュータからユーザコンピュータに送信される所定の情報に基づいて、第2のソフトウェアをデコードするステップと、認証用コンピュータから受信した所定の情報に基づいて、第2のソフトウェアを起動させるための起動情報を生成させるステップと、生成された起動情報によって第2のソフトウェアを起動させるステップと、起動された第2のソフトウェアの実行を監視し、第2のソフトウェアの実行が終了した場合は、第2のソフトウェアを無力化させるステップと、を含んでなるソフトウェアの更新方法。

本発明の他の観点に従う管理用コンピュータは、アプリケーションソフトウェア及び監視プログラムと共にユーザコンピュータにインストールされる実行制御プログラムと通信を行うことにより、実行制御プログラムの動作を制御するものである。そして、この管理用コンピュータは、実行制御プログラムからの要求に基づいてユーザ認証を行う認証部と、認証部により正当なユーザであると確認された場合は、実行制御プログラムがアプリケーションソフトウェアを起動させるために必要な第1の情報を実行制御プログラムに送信する情報送信部と、所定の時期に実行制御プログラムとの間で行われる継続確認通信に基づいて、アプリケーションソフトウェアの実行継続を許可するか否かを管理する継続実行管理部と、を備えている。

本発明の一態様では、継続実行管理部は、継続確認通信によって実行制御プログラムから取得される第1の識別情報とユーザ認証に予め関連付けられている第2の識別情報とを比較し、両方の識別情報が対応する場合は、実行制御プログラムに対してアプリケーションソフトウェアの実行継続を許可し、各識別情報が対応していない場合は、実行制御プログラムに対してアプリケーションソフトウェア

アの実行継続を禁止させる。

本発明の一態様では、継続実行管理部は、第2の識別情報に対応する第1の識別情報を予め実行制御プログラムに設定させる。

本発明の一態様では、継続実行管理部は、所定の時期を実行制御プログラムに
5 予め設定し、この予め設定された所定の時期が到来した場合は、実行制御プログラムから継続実行管理部に対して継続確認通信を行わせる。

本発明の一態様では、継続実行管理部は、所定の時期を可変に設定可能となっている。

本発明の一態様では、継続実行管理部は、少なくとも予測される将来の負荷状
10 態を考慮して、所定の時期を可変に設定可能である。

本発明の一態様では、監視プログラムは、アプリケーションソフトウェア及び
実行制御プログラムの動作状態をそれぞれ監視し、アプリケーションソフトウェア
または実行制御プログラムのいずれか一方が動作を停止した場合は、アプリ
ケーションソフトウェア及び実行制御プログラムをそれぞれ停止させ、自身も停止
15 させるものであり、実行制御プログラムは、アプリケーションソフトウェア及び
監視プログラムの動作状態をそれぞれ監視し、アプリケーションソフトウェアま
たは監視プログラムのいずれか一方が動作を停止した場合は、アプリケーション
ソフトウェア及び監視プログラムをそれぞれ停止させ、自身も停止させるもので
ある。

20 本発明のさらに別の観点に従うコンピュータプログラムは、コンピュータを、
アプリケーションソフトウェアの実行を制御する実行制御部と、アプリケーショ
ンソフトウェア及び実行制御部の動作状態をそれぞれ監視する監視部として、機
能させるものであって、実行制御部は、管理用コンピュータと通信することによ
りユーザ認証を要求する機能と、管理用コンピュータから受信した第1の情報に
25 基づいて、アプリケーションソフトウェアを起動させる機能と、管理用コンピュ

ータとの間で継続確認通信を行う機能と、継続確認通信によってアプリケーションソフトウェアの実行継続が禁止された場合は、アプリケーションソフトウェアの動作を停止させる機能と、を備え、監視部は、アプリケーションソフトウェア及び実行制御部の動作状態をそれぞれ監視する機能と、アプリケーションソフトウェアまたは実行制御部のいずれか一方が動作を停止した場合は、アプリケーションソフトウェア及び実行制御部をそれぞれ停止させ、自身も停止させる機能と、を備えている。

10

図面の簡単な説明

図1は、本発明の実施形態に係るソフトウェア実行制御システムの全体概要を示す説明図である。

図2は、データベース等の構造を示し、(a)はユーザ情報データベースを、(b)はゲーム情報データベースを、(c)はHTMLヘッダ内に暗号化された起動情報を埋め込んで送信する様子を、それぞれ示す。

図3は、プログラムの概略構造を示し、(a)はゲームプログラムを、(b)は実行制御プログラムの構造を、それぞれ示す。

図4は、ユーザコンピュータにインストールされた旧版のゲームプログラムを、新版のゲームプログラムに更新し、起動を制御する様子を示す説明図である。

図5は、ゲームプログラム及び実行制御プログラムをインストールするときの処理を示すフローチャートである。

図6は、実行制御プログラム及び認証用コンピュータとの間で行われるオンライン認証等を示すフローチャートである。

25 図7は、

本発明の他の実施形態に係るソフトウェア実行制御システムの全体概要を示す説明図である。

図 8 は、データベース等の構造を示し、(a) はユーザ情報データベースを、(b) はゲーム情報データベースを、(c) は監視状況データベースを、それぞれ示す。

5 図 9 は、ソフトウェア実行制御システムの全体動作の概要を示すフローチャートである。

図 10 は、周期的に行われる継続確認通信の処理概要を示すフローチャートである。

図 11 は、次回の継続確認通信を行う時期を決定する処理の概要を示すフロー
10 チャートである。

図 12 は、ゲームマネージャ及び監視プログラムがそれぞれ相互に監視する処理の概要を示すフローチャートである。

図 13 は、本発明のさらに別の実施形態に係るソフトウェア実行制御システムの全体概要を示す説明図である。

15

発明を実施するための最良の形態

以下、本発明の実施形態を図 1 ～図 13 を参照しつつ詳細に説明する。

20 まず、図 1 ～図 6 に基づいて第 1 実施例を説明する。図 1 は、ソフトウェア実行制御システムの全体概要を示す説明図である。本実施例では、ゲームプログラムをオンラインで更新させるシステムを例に挙げて説明する。

配信用コンピュータ 10 は、新版のゲームプログラム 40 及び実行制御プログラム 50 を、インターネット等の通信ネットワークを介して、各ユーザのコンピュータ 30 に配信するためのものである。配信用コンピュータ 10 は、各ソフト
25

ウェア会社（ベンダー）毎にそれぞれ設置されるサーバとして構成することができる。

まず、配信用コンピュータ 10 は、ゲームプログラムデータベース 12 に登録された新版プログラムについて、事前に、認証用コンピュータ 20 に登録を行う（S1）。例えば、新版ゲームプログラムの名称、種類、販売価格、データサイズ、バージョン情報等のデータが、配信用コンピュータ 10 から認証用コンピュータ 20 に登録される。もっとも、配信用コンピュータ 10 と認証用コンピュータとが一体的に構成されている場合は、このような外部ネットワークを介した通知は必ずしも必要ない。

10 配信用コンピュータ 10 の配信制御部 11 は、ユーザコンピュータ 30 からプログラムの更新要求を受けると、ユーザの希望するゲームプログラム 40 をゲームプログラムデータベース 12 から読み出して、ユーザコンピュータ 30 に配信するようになっている（S2）。ここで、新版のゲームプログラム 40 は、単独でユーザコンピュータ 30 に配信されるのではなく、ゲームプログラム 40 の起動
15 や削除等を管理する実行制御プログラム 50 と共にユーザコンピュータ 30 に配信される点に留意すべきである。

認証用コンピュータ 20 は、例えば、複数のソフトウェア会社が所属する団体や機関毎にそれぞれ設置されるサーバとして構成することができる。また、これに限らず、各ソフトウェア会社毎に認証用コンピュータ 20 をそれぞれ設置して
20 もよい。認証用コンピュータ 20 は、認証部 21 と、課金処理部 22 と、起動情報送信部 23 と、ユーザ情報データベース 24 と、ゲーム情報データベース 25 とを備えている。

認証部 21 は、ユーザコンピュータ 30 の実行制御プログラム 50 から送信される所定の認証用データに基づいて、ユーザ認証を行うものである。詳細は後述
25 するが、認証用データには、例えば、ユーザ識別情報（ユーザ ID）、パスワード

(PW)、MAC アドレス (Media Access Control address) が含まれる。

課金処理部 22 は、新版ゲームプログラム 40 の使用許諾に際して、ユーザに課金するものである。課金方法には、種々のものを採用できる。例えば、ゲームプログラムの代金を一括でユーザに支払わせたり (売り切り)、又は、ユーザがゲームプログラムを使用する毎に課金してもよい。あるいは、所定期間や所定回数
5 毎に課金するようにしてもよい。なお、支払方法も、例えば、クレジット決済、電子マネー決済等のように種々のものを採用できる。

起動情報送信部 23 は、ユーザコンピュータ 30 の記憶装置 (例えば、ハードディスク等) に格納された新版のゲームプログラム 40 をデコードし、起動させるために必要な起動情報をユーザコンピュータ 30 の実行制御プログラム 50 に
10 向けて送信するものである。

ユーザが、実行制御プログラム 50 を介して認証用コンピュータ 20 の認証部 21 と認証を行い、ゲームプログラム 40 の購入代金 (使用権の代金) を支払い済みの正当なユーザであると認証された場合は (S3)、起動情報送信部 23 から
15 起動情報が実行制御プログラム 50 に送信される (S4)。ゲームプログラム 40 の代金を未払いのユーザが認証用コンピュータ 20 にアクセスした場合は、課金処理部 22 を介して課金処理が行われた後、起動情報が実行制御プログラム 50 に向けて送信される。

さて、ユーザコンピュータ 30 の構成に目を転じると、ユーザコンピュータ 30
20 は、例えば、パーソナルコンピュータ、ワークステーション、携帯情報端末、携帯電話等のコンピュータとして構成されている。ユーザコンピュータ 30 は、演算処理装置 (CPU)、主記憶、補助記憶、外部入出力回路等のコンピュータ資源を必要に応じて備えており、これらの各資源は適宜ゲームプログラム 40 及び
実行制御プログラム 50 によって使用される。

25 配信用コンピュータ 10 からユーザコンピュータ 30 に送信された新版のゲー

ムプログラム 40 及び実行制御プログラム 50 は、後述のように、付属するインストーラによってユーザコンピュータ 30 にインストールされる。そして、実行制御プログラム 50 が認証用コンピュータ 20 との間でユーザ認証を行い、起動情報を入手すると、ゲームプログラム 40 が起動される (S5)。なお、新版のゲームプログラム 40 をインストールするより前に、ユーザコンピュータ 30 に既にインストールされていた旧版のゲームプログラムは、新版のプログラムに置き換えられるため、以後使用することができなくなる。

ユーザは、ユーザコンピュータ 30 を介して新版のゲームプログラム 40 を利用することができる。そして、ユーザがゲームを終えて、ゲームプログラム 40 を終了させると、実行制御プログラム 50 は、ゲームプログラム 40 を削除する等して無力化する (S6)。ユーザがゲームプログラム 40 を再び利用する場合は、認証用コンピュータ 20 に再度アクセスしてユーザ認証を行い、起動情報を取得する。

ここで、ユーザコンピュータ 30 の記憶装置内には、新版のゲームプログラム 40 がデコード前の暗号化ファイルの状態で作成されているため、ゲームプログラム 40 を再使用する場合は、この暗号化ファイルをデコードするための情報 (デコードキー) と起動させるための情報とを認証用コンピュータ 20 から取得するだけでよい。即ち、本実施例では、ユーザコンピュータ 30 のローカルディスクに新版ゲームプログラム 40 を暗号化ファイルの状態で作成しておき、ゲームを行うたびに、認証用コンピュータ 20 との間でオンライン認証を行って、暗号化されたゲームプログラム 40 をデコードして起動させる。そして、ゲーム終了後には、デコードされたゲームプログラム 40 を削除して無力化させる。

次に、図 2 は、認証用コンピュータ 20 が利用するユーザ情報データベース 24 及びゲーム情報データベース 25 の構造例を示す説明図である。なお、図 2 に示す各データベース 24, 25 の内容は一例であって、図示する項目の全てを備

える必要はない。

図2(a)に示すユーザ情報データベース24は、例えば、ユーザIDと、パスワードと、複数のMACアドレス1～nと、購入済のゲームプログラムを特定するゲームID1～nと、その他の情報とをそれぞれ対応付けることにより構成5 されている。ここで、複数のMACアドレス1～nを登録可能としたのは、1人のユーザがそれぞれ異なる複数のユーザコンピュータ30を用いて、ゲームプログラム40を使用する場合も考慮したためである。従って、ユーザは、例えば、職場のコンピュータ、自宅のコンピュータ等の異なる情報処理端末を介して、ゲームプログラム40を利用できるようになっている。その他の情報としては、例10 えば、ユーザの氏名、年齢、住所、ゲームのプレイ回数、獲得したポイント数(例えば、ゲーム購入代金やプレイ回数等に応じてポイントを与えるような場合)等を挙げることができる。

図2(b)に示すゲーム情報データベース25は、例えば、ゲームIDと、ゲーム名と、ゲーム情報(ゲームプログラムのレジストリパスを示す情報)と、暗15 号化されたゲームプログラム40を復号するためのデコードキーと、デコードされたゲームプログラム40を起動させるための起動引数と、その他の情報とをそれぞれ対応付けることにより構成されている。その他の情報としては、例えば、ゲームの種類(ロールプレイングゲーム、格闘ゲーム、成人指定の有無等)、データサイズ、著作権管理情報等を挙げることができる。

20 図2(c)に示すように、ゲーム情報、デコードキー及び起動引数は、暗号化されてHTML(Hyper Text Markup Language)データに埋め込まれ、ユーザコンピュータ30に送信されるようになっている。即ち、ユーザコンピュータ30側で生成された暗号化キー及びMACアドレスによって、起動情報(ゲーム情報、デコードキー、起動引数)は暗号化され、例えば、HTMLのヘッダ部に埋め込25 まれる。従って、認証用サーバ20は、ユーザコンピュータ30からのHTTP

(Hyper Text Transport Protocol) リクエストに応じて、暗号化された起動情報を生成し、この暗号化された起動情報を含んだ HTTP レスポンスをユーザコンピュータ 30 に返すようになっている。

次に、図 3 は、ゲームプログラム 40 及び実行制御プログラム 50 の概略構成 5 を示す説明図である。

図 3 (a) に示すように、ゲームプログラム 40 は、プログラム本体 41 と、付随データ群 42 とを含んでいる。付随データ群 42 としては、例えば、動画像データ、静止画像データ、グラフィックスデータ、楽曲データ、音声データ、テキストデータ等を挙げることができる。

- 10 新版のゲームプログラム 40 は、旧版のプログラムに比較して、プログラム 41 又は付随データ群 42 のいずれか又は双方が新しく作成されている。プログラム本体 41 及び付随データ群 42 の両方が旧版よりも新しい場合は、プログラム本体 41 及び付随データ群 42 の両方が新版に置き換えられる。付随データ群 42 のみが新しい場合及びプログラム本体 41 のみが新しい場合は、付随データ群
15 42 又はプログラム本体 41 のいずれかが新版に置き換えられる。

図 3 (b) に示すように、実行制御プログラム 50 は、ユーザコンピュータ 30 上で、暗号用情報生成部 51 と、認証要求部 52 と、ゲーム選択部 53 と、暗号解読部 54 と、起動部 55 と、デコード部 56 と、実行監視部 57 という各機能を実現させる。一例として、実行制御プログラム 50 は、デバイスを特定しな
20 いデバイスドライバとして構成されている。このため、実行制御プログラム 50 は、例えば、ゲームプログラム等のアプリケーションプログラムとは異なって、タスク管理プログラム等から終了させることができないように構成することができる。

暗号情報生成部 51 は、例えば、ユーザコンピュータ 30 の内蔵タイマから取
25 得した時刻情報に基づいて暗号化キーを生成するほか、ユーザコンピュータ 30

の MAC アドレス等を取得する。

認証要求部 5 2 は、ユーザコンピュータ 3 0 に実装されているネットワークアクセスの機能を内部的に呼び出して、認証用コンピュータ 2 0 にアクセスし、暗号化キー、MAC アドレス、ユーザ ID 及びパスワードを認証用コンピュータ 2 5 0 に送信してユーザ認証を求める。

ゲーム選択部 5 3 は、ユーザ認証が終了して認証用コンピュータ 2 0 からユーザコンピュータ 3 0 に送信された一覧メニューから、ユーザが希望するゲームを選択させる。この一覧メニューは、ユーザが利用可能な（起動可能な）ゲームプログラムを一覧形式で表示させるものであり、ユーザ情報データベース 2 4 の購入済ゲーム ID に基づいて生成することができる。

暗号化情報生成部 5 1 によって生成された暗号化キー及び MAC アドレスにより、ユーザの選択したゲームプログラム 4 0 を起動させるための起動情報は、暗号化されてユーザコンピュータ 3 0 に送信される。暗号解読部 5 4 は、暗号化キー及び MAC アドレスに基づいて、暗号化された起動情報を解読する。

15 デコード部 5 6 は、解読されたデコードキーによって、暗号化されたゲームプログラム 4 0 をデコードさせる。なお、暗号化ファイルはそのまま保存される。起動部 5 5 は、解読されたゲーム情報及び起動引数に基づいて、起動ステートメントを生成し、デコードされたゲームプログラム 4 0 を起動させる。起動ステートメントは、ゲームプログラムのレジストリパスと起動引数から構成される。

20 ゲームプログラム 4 0 が起動されると、実行監視部 5 7 は、ゲームプログラム 4 0 の実行状態を監視し、ゲームプログラム 4 0 が終了すると、デコードされたプログラム本体 4 1 を削除する。なお、デコードした付随データ群も一緒に削除してもよい。また、削除する場合は、プログラム又はデータの全部を削除してもよいし、一部を削除してもよい。

25 次に、図 4 は、本システムによってゲームプログラムを最新版に更新する様子

を模式的に示す説明図である。

まず、図4(a)に示すように、ユーザコンピュータ30には、旧版のゲームプログラムが既にインストールされている。なお、図中では、バージョンアップ前の旧版のゲームプログラムを「初期プログラム」と、バージョンアップする新5 版のゲームプログラムを「更新版プログラム」とそれぞれ表示する。

ユーザは、例えば、CD-ROM、DVD-ROM、メモリ等の記録媒体に固定された旧版のゲームプログラム40Aをユーザコンピュータ30にインストールして利用する(S11)。あるいは、インターネット等の通信ネットワークを介して旧版10 のゲームプログラム40Aを取得することもできる。この旧版のゲームプログラ
ム40Aは、認証用コンピュータ20とのオンライン認証を受けることなく使用可能である。但し、本更新システムによっていったん更新された後は、更新版プログラムが旧式になった場合でも、オンライン認証を受けなければ利用することはできない。

旧版のゲームプログラム40Aを利用するユーザには、新版ゲームプログラム15 40へアップデート可能である旨が通知される。この通知は、種々の方法で行うことができる。

第1の方法は、例えば、旧版のゲームプログラム40Aが、積極的又は消極的に、ユーザに新版のゲームプログラム40へ更新可能であることを通知し、併せて、配信用コンピュータ10のURL(Uniform Resource Locator)を表示する方20 法である。積極的な通知としては、例えば、ゲーム開始時や終了時等に更新可能である旨及び配信用コンピュータ10のURLを画面に表示させることが考えられる。消極的な通知としては、例えば、旧版のゲームプログラム40Aのヘルプメニューの中に、更新可能である旨及び配信用コンピュータ10のURLを表示させることが考えられる。いずれの場合も、URLをクリックするだけで、ウェブ25 ブラウザ31を起動させ、自動的にユーザコンピュータ30を配信用コンピュ

ータ 10 にアクセスさせるように構成すると、ユーザの使い勝手が良い。

第 2 の方法は、電子的な媒体を介して積極的又は消極的に、新版のゲームプログラム 40 へ更新可能である旨及び配信用コンピュータ 10 の URL を、ユーザに通知する方法である。積極的な通知としては、例えば、ユーザ宛の電子メール 5 を挙げることができる。消極的な通知としては、例えば、ウェブ上のサイト（例えば、配信用コンピュータ 10 等）で、新版のゲームプログラム 40 を広告宣伝することが考えられる。

第 3 の方法としては、その他、ゲーム雑誌やコンピュータ雑誌等の紙媒体上で 10 の広告宣伝、ネットワーク上に形成されたゲームプログラム同好会のようなコミ

以上のようにして、ユーザに対し、新版ゲームプログラム 40 の存在を通知させることができる。図 4 (b) に示すように、更新を希望するユーザは、ウェブブラウザ 31 を介して配信用コンピュータ 10 にアクセスし、新版ゲームプログラム 40 への更新を要求する (S12)。

15 図 4 (c) に示すように、配信用コンピュータ 10 は、ユーザの希望する新版のゲームプログラム 40 (付随データ群も含まれる) を、通信ネットワークを介して、ユーザコンピュータ 30 に向けて送信する (S13)。また、新版のゲームプログラム 40 と一緒に実行制御プログラム 50 もセットにしてユーザコンピュータ 30 に送信される (S13)。新版のゲームプログラム 40 及び実行制御プログラム 50 は、ユーザコンピュータ 30 の記憶装置に保存される。

新版のゲームプログラム 40 及び実行制御プログラム 50 には、専用のインストーラが付属している。インストーラにより、新版のゲームプログラム 40 及び実行制御プログラム 50 がユーザコンピュータ 30 にインストールされる。実行制御プログラムが起動すると、図 4 (d) に示すように、実行制御プログラム 5 25 0 は、ネットワークアクセスの機能呼び出して、認証用コンピュータ 20 にア

クセスし、認証用コンピュータ 20 との間で、ユーザ認証及び購入処理（課金処理）を行う（S14）。ユーザ認証や課金処理を終えた後で、認証用コンピュータ 20 は、ユーザコンピュータ 30 の実行制御プログラム 50 に向けて、暗号化された起動情報を送信する（S15）。

5 実行制御プログラム 50 は、暗号化された起動情報を解読して、デコードキーや起動引数等を取り出す。そして、実行制御プログラム 50 は、ゲームプログラム 40 をデコードして起動させる。これにより、ユーザは、新版のゲームプログラム 40 を利用することができる。ゲームプログラム 40 の実行状態は、実行制御プログラム 50 により監視される。

10 図 4（e）に示すように、ユーザがゲームプレイを終了し、ゲームプログラム 40 が終了すると、実行制御プログラム 50 は、新版のゲームプログラム 40 を削除することにより無力化させる（S16）。

一例として、デコードされて実行可能な状態（起動ステートメントの入力により起動可能な状態）に置かれている新版のゲームプログラム 40 のみを削除し、

15 配信用コンピュータ 10 から取得したデコード前の暗号化ファイルは、ユーザコンピュータ 30 の記憶装置内に保存しておくことができる。

これにより、ユーザがゲームプログラム 40 の再プレイを希望する場合は、認証用コンピュータ 20 にアクセスしてオンラインによるユーザ認証を受け、認証用コンピュータ 20 から起動情報を改めて取得するだけで足りる（S17）。暗号

20 化されたゲームプログラム 40 を配信用コンピュータ 10 から改めて取得する必要がないため、ダウンロードの手間がかからず、また通信ネットワークへの負担を軽減することができる。

このように、ゲームプログラム 40 を再度プレイする場合は、ゲームプログラム 40 の起動情報のみを再取得する方法が便利であるが、本発明はこれに限らず、
25 デコード前の暗号化されたプログラムを配信用コンピュータ 10 から再度取得す

るようにしてもよい。また、デコードされたプログラム本体 4 1 のみを削除し、付随データ群 4 2 をそのまま残してもよい。

次に、図 5 及び図 6 に基づいて、本システムの処理の詳細を説明する。図に示すフローチャートは、処理の大まかな流れを示すものであり、実際のプログラム 5 とは相違する。

図 5 は、ユーザコンピュータ 3 0 の記憶装置に格納された新版のゲームプログラム 4 0 及び実行制御プログラム 5 0 をインストール等する処理を示す。

ゲームプログラム 4 0 及び実行制御プログラム 5 0 は暗号化ファイルの状態でユーザコンピュータ 3 0 に保存される。例えば、ユーザが、暗号化ファイルをマウスポインタで選択してダブルクリックする等のように、起動イベントを発生させると、インストーラが起動する (S 2 1)。

インストーラは、ユーザコンピュータ 3 0 に更新すべき旧版のゲームプログラム 4 0 A がインストール済であるか否かを判定する (S 2 2)。旧版のゲームプログラム 4 0 A がインストールされていない場合は、例えば、「旧版のゲームがインストールされていません。処理を終了します。」等のような警告メッセージを画面 15 に表示させて終了する (S 2 3)。

旧版のゲームプログラム 4 0 A がユーザコンピュータ 3 0 にインストールされている場合は (S22:YES)、新版のゲームプログラム 4 0 及び実行制御プログラム 5 0 を初めてインストールするの否かを判定する (S 2 4)。新版ゲームプログラム 4 0 及び実行制御プログラム 5 0 が過去にインストールされている場合は、既にユーザ登録及び課金処理が完了しているものとみなすことができる。従って、S 2 4 は、結果的に、既にユーザ登録及び課金処理が完了しているか否かを判定することになる。

初めてのインストールである場合は、ウェブブラウザ 3 1 の機能呼び出して 25 認証用コンピュータ 2 0 に接続し、ユーザに、ユーザ登録及び課金処理を行わせ

る (S 25, S 26)。

次に、インストーラは、実行制御プログラム 50 のレジストリを判定し、実行制御プログラム 50 が未だインストールされていない場合は、実行制御プログラム 50 をインストールする (S 27)。インストーラは、旧版のゲームプログラム 540A を新版のゲームプログラム 40 に置き換えて更新すべく、旧版のプログラム本体 41 及び付随データ群 42 を新版のプログラム本体 41 及び付随データ群 42 に書き換える (S 28, S 29)。そして、インストーラは、実行制御プログラム 50 を起動させて処理を終了する (S 30)。

図 6 は、実行制御プログラム 50 による実行制御処理及び認証用コンピュータ 1020 の処理等を示すフローチャートである。

起動された実行制御プログラム 50 は、ユーザコンピュータ 30 に固有のマシン情報、具体的には、MAC アドレスを取得する (S 41)。また、ユーザコンピュータ 30 の内蔵タイマから現在時刻の情報を取得し、この時刻情報に基づいて暗号化キーを生成する (S 42)。

15 次に、実行制御プログラム 50 は、ウェブブラウザ 31 の機能呼び出し (S 43)、通信ネットワークを介して認証用コンピュータ 10 に接続し、認証用コンピュータ 20 にログイン認証を要求する (S 44)。実行制御プログラム 50 は、ユーザ ID、パスワード、MAC アドレス及び暗号化キーを認証用コンピュータ 20 に送信する (S 44)。認証用コンピュータ 20 は、ユーザ情報データベース 2024 を参照し、正当なユーザであるか否かを判断する (S 61)。

正当なユーザであると認められた場合、認証用コンピュータ 20 は、ユーザが利用可能なゲームプログラムの一覧データを作成し、ユーザコンピュータ 30 に送信する (S 62)。ユーザが利用することができるゲームプログラムとしては、典型的には、そのユーザが購入しているゲームプログラムを挙げることができる
25 が、これに限らず、例えば、ソフトウェア会社が無償で提供しているゲームプロ

グラム等を含めることもできる。

実行制御プログラム50は、利用可能なゲームプログラムの一覧データを認証用コンピュータ20から受信すると、ユーザコンピュータ30のモニタディスプレイにゲームの一覧を表示させる（S45）。この一覧メニューに基づいて、ユーザは、プレイを希望するゲームを選択する（S46）。

認証用コンピュータ20は、ゲーム情報データベース25を参照して、ユーザが選択したゲームプログラムを起動させるために必要な起動情報を生成し、この起動情報を、S61で取得した暗号化キー及びMACアドレス等によって暗号化する（S63）。認証用コンピュータ20は、暗号化された起動情報をユーザコンピュータ30の実行制御プログラム50に送信する（S64）。

実行制御プログラム50は、暗号化された起動情報を認証用コンピュータ20から受信すると（S47）、この暗号化された起動情報を暗号化キー及びMACアドレスによって解読する（S48）。

次に、実行制御プログラム50は、新版のゲームプログラム40のレジストリ情報を取得し（S49）、レジストリパスと起動引数とによって起動ステートメントを生成する（S50）。

また、実行制御プログラム50は、起動情報から取り出したデコードキーによって、暗号化された新版のゲームプログラム40をデコードし、所定のドライブの所定のディレクトリに展開させる（S51）。これにより、ゲームプログラム40はデコードされて起動待ちの状態になる。

そして、実行制御プログラム50は、S50で生成した起動ステートメントによって、デコードされた新版のゲームプログラム40を起動させる（S52，S70）。これにより、ユーザは、新版のゲームプログラム40で遊ぶことができる（S71）。

実行制御プログラム50は、ゲームプログラム40の実行状態を監視しており

(S 5 3)、ユーザがゲームを終えてゲームプログラム 4 0 を終了させた場合には (S 7 2)、デコードされたプログラム本体 4 1 を削除等することにより、ゲームプログラム 4 0 を無力化し、処理を終了する (S 5 4)。

5 なお、ユーザが再びゲームプログラム 4 0 で遊びたい場合は、再度認証用コンピュータ 2 0 にアクセスしてオンラインによる認証を受け、起動情報を取得すればよい。

このように構成される本実施例によれば、ユーザコンピュータ 3 0 にプログラムを格納させるダウンロード式のソフトウェア配信の場合でも、使用権を購入していない違法な使用を阻止することができる。

10 即ち、本実施例において、ゲームプログラム 4 0 を起動させるには、使用する度毎に、実行制御プログラム 5 0 を介してオンラインによる認証を行い、認証用コンピュータ 2 0 から通信ネットワークを介して起動情報を取得する必要があるため、仮に、ゲームプログラム 4 0 のみを単体で違法にコピーしても、違法にコピーされたゲームプログラム 4 0 を単体で起動させることはできない。

15 また、実行制御プログラム 5 0 はデバイスドライバのように OS 側に近いプログラムとして構成されており、アプリケーションプログラムのように通常の方法では終了させることができない。従って、実行制御プログラム 5 0 とゲームプログラム 4 0 とを切り離して、ゲームプログラム 4 0 のみを違法にコピーしたり持ち出したりすることができないようになっている。

20 本発明は、種々のビジネスに活用することができるであろう。例えば、過去に違法にコピーされて流通している旧版ゲームプログラムを、新版ゲームプログラムに更新させることにより、違法使用のユーザに正式に使用権を取得させて、正当なユーザへ変えることができる。違法なユーザを新版のゲームプログラムに乗り換えさせるためには、そのユーザの母国語に対応した付随データ群 (ゲームシ
25 ナリオや楽曲等) を用意したり、追加のシナリオ等を新しく用意したりして、ユ

ーザの更新意欲を刺激すればよい。

次に、図 7～図 12 を参照し、他の実施例を説明する。本実施例では、ゲームプログラムを記録媒体に固定して流通させる場合を例に挙げて説明する。本実施
5 例では、本発明の範囲を減縮しない限りにおいて、前記実施例で述べた説明を適宜援用することができる。後述のように本実施例では、上記実施例と同様に、実行制御プログラム（本実施例のゲームマネージャ）によってゲームプログラムの実行を制御している。これに加えて、本実施例では、認証用コンピュータ（本実施例の DRM コンピュータ）と実行制御プログラムとの間のオンライン認証を、
10 定期的に実行可能としている。

図 7 は、本実施例によるソフトウェア実行制御システムの全体概要を示す説明図である。本システムは、それぞれ後述するように、例えば、サプライヤコンピュータ 100 と、DRM コンピュータ 200 と、ユーザコンピュータ 300 とを含めて構成することができる。

15 サプライヤコンピュータ 100 は、例えば、プログラムプロダクトを生産するソフトウェアベンダーにより使用される。サプライヤコンピュータ 100 は、ゲームプログラム 400 を加工して DRM 化プログラム 700 に変換する DRM 部 110 を備えている。ここで、DRM とは、Digital Rights Management の略称であり、ゲームプログラム等のデジタル化されたコンテンツの権利を管理すること
20 を意味する。本明細書において、DRM 化とは、ノンプロテクトのゲームプログラムに後述する独自のプロテクトを設定することにより、不正使用等に対する耐性を向上させることを意味する。

DRM 部 110 は、ゲームプログラム 400 に、ゲームマネージャ 500 及び監視プログラム 600 を加えることにより、ゲームプログラム 400 に独自の
25 プロテクトを設定する。プロテクトされたゲームプログラム 400 は、DRM 化プ

プログラム700として、記録媒体RMに記録され市場に流通する。ゲームマネージャ500及び監視プログラム600については、さらに後述する。

記録媒体RMとしては、例えば、CD-ROM、DVD-ROM、光ディスク、ハードディスク、フレキシブルディスク、半導体メモリ、磁気テープ等のような種々の媒体を適宜用いることができる。DRM化プログラム700を圧縮して記録媒体RMに記録してもよいし、DRM化プログラム700を圧縮することなく記録媒体RMに記録してもよい。また、記録媒体RMには、DRM化プログラム700をユーザコンピュータ300にインストールさせるためのインストーラを記憶させることもできる。

- 10 DRMコンピュータ200は、「管理コンピュータ」の一例である。DRM化コンピュータ200は、例えば「認証管理サーバ」等と呼ぶこともできる。DRM化コンピュータ200は、各ソフトウェアベンダー毎にそれぞれ設置してもよいし、複数のソフトウェアベンダーに対して1つだけ設置してもよい。

DRMコンピュータ200は、ユーザコンピュータ300上で稼働するゲーム
15 マネージャ500との間で通信を行うことにより、ユーザ認証、起動情報の送信、及び継続実行の管理を行うものである。DRMコンピュータ200は、認証部210と、起動情報送信部220と、継続実行管理部230とを備えている。

また、DRMコンピュータ200は、ユーザ情報データベース240と、ゲーム情報データベース250と、監視状況データベース260とを利用することが
20 できる。なお、DRMコンピュータ200は、物理的に単一のコンピュータから構成されている必要はなく、複数のコンピュータの協働動作によって実現されてもよい。

認証部210は、前記実施例の認証部21と同様に、例えば、ユーザID、パスワード（図中「PW」）ゲームマネージャ500から送信される認証用データに
25 基づいて、ユーザ認証を行うものである。起動情報送信部220は、前記実施例

の起動情報送信部 23 と同様に、例えば、ゲームマネージャ 500 がゲームプログラム 400 をデコードして起動可能状態に置くために必要な情報を、ゲームマネージャ 500 に送信するものである。

継続実行管理部 230 は、ゲームマネージャ 500 との間で所定時間毎に通信 5 を行うことにより、ゲームプログラム 400 の実行継続の可否を管理するものである。詳細はさらに後述するが、継続実行管理部 230 は、ゲームマネージャ 500 から送信されたセッション ID と予め保持されているセッション ID とを比較し、両者が一致する場合は、ゲームプログラム 400 の実行継続を許可する。逆に、継続実行管理部 230 は、両セッション ID が一致しない場合、ゲームプログラム 400 の強制終了をゲームマネージャ 500 に対して指示する。

ユーザコンピュータ 300 は、前記実施例のユーザコンピュータ 3 と同様に、例えば、パーソナルコンピュータや携帯情報端末、携帯電話等として構成可能なものである。ユーザコンピュータ 300 は、CPU、メモリ、補助記憶装置、OS、各種デバイスドライバ等のように、ハードウェア資源及びソフトウェア資源 15 を必要に応じて備えることができる。ゲームプログラム 400 と、ゲームマネージャ 500 と、監視プログラム 600 とは、ユーザコンピュータ 300 の有するハードウェア資源及びソフトウェア資源を適宜利用することができる。

記録媒体 RM の記憶内容をユーザコンピュータ 300 に読み込ませ、所定のインストール処理を行うことにより、ユーザコンピュータ 300 上でゲームプログラム 400、ゲームマネージャ 500 及び監視プログラム 600 がそれぞれ実行 20 される。正当な権限を有するユーザにとって、ゲームマネージャ 500 はゲームプログラム 400 を起動させるためのランチャープログラムとして作用する。しかし、ゲームマネージャ 500 は、単なるランチャープログラムではなく、ゲームプログラム 400 の作動を制御する。また、ゲームマネージャ 500 は、ゲームプログラム 400 及び監視プログラム 600 の動作状態をそれぞれ監視し、い 25

いずれか一方の監視対象が動作を停止した場合は、他方の監視対象及び自身の動作を停止させる。

監視プログラム600は、ゲームプログラム400及びゲームマネージャ500の動作状態をそれぞれ監視し、いずれか一方の監視対象が動作を停止した場合は、他方の監視対象及び自身の動作を停止させる。正当なユーザは、監視プログラム600の存在を意識せずに、ゲームプログラム400を使用することができる。

図8は、各データベース240～260の一例を示す説明図である。図8(a)に示すように、ユーザ情報データベース240は、例えば、ユーザIDと、パスワードと、MACアドレスと、セッションIDと、その他の情報とを対応付けて管理することができる。後述のように、セッションIDは、継続実行を許可するか否かを判定するために用いられる情報である。即ち、最初に認証されたユーザコンピュータ300とは別のユーザコンピュータを使用してゲームプログラム400が不正に実行されるのを防止するために、ゲームマネージャ500とDRMコンピュータ200とは定期的に通信を行う。この際に、ゲームマネージャ500から受信したセッションIDと、ユーザ情報データベース240に登録されているセッションIDとの比較が行われ、セッションIDが一致する場合にのみゲームプログラム400の実行継続が許可されるようになっている。なお、図2(a)に示すユーザ情報データベース24と同様に、1つのユーザIDに複数のMAC
20 アドレスを対応付けることもできる。

図8(b)に示すように、ゲーム情報データベース250は、例えば、ゲームIDと、ゲーム名と、ゲーム情報と、デコードキー(アクティバイトキー)と、起動引数と、報告モードとを対応付けて管理することができる。ここで、報告モードとは、ゲームマネージャ500からDRMコンピュータ200への定期的な
25 報告の頻度に関する方針を設定する情報である。報告モードは、例えば、ゲーム

プログラム４００の提供者（ソフトウェアベンダー）が設定することができる。

ここで、報告モードとしては、例えば、ゲームプログラム４００を最初に起動した時だけＤＲＭコンピュータ２００に報告するモードと、ゲームプログラム４００を起動させる度にＤＲＭコンピュータ２００に報告するモードと、監視効率を優先して可能な限り短周期でＤＲＭコンピュータ２００に報告するモードと、

５ ＤＲＭコンピュータ２００の負荷低減を考慮して少ない頻度でＤＲＭコンピュータ２００に報告するモードと、を挙げることができる。

図８（ｃ）に示すように、監視状況データベース２６０は、例えば、ゲームプログラム４００を実行している各ユーザのユーザＩＤと、各ユーザコンピュータ

１０ ３００からの報告周期と、次回の報告時期と、各ユーザが実行しているゲームプログラム４００のゲームＩＤと、ゲームスタート時刻とを対応付けて管理することができる。後述のように、次回の報告時期は、ＤＲＭコンピュータ２００の負荷状態や報告モード等に基づいて動的に制御される。

次に、図９～図１２に基づいて、本システムの動作を説明する。まず、図９は、

１５ 本システムの起動時に行われる動作の概要を示すフローチャートである。

ゲームプログラム４００の利用を希望するユーザは、例えば、所望のゲームプログラム４００を象徴するゲームアイコンを選択し、起動を指示する。このユーザによる操作が検出されると、まず最初に、ゲームマネージャ５００が起動する（Ｓ１０１）。

２０ ゲームマネージャ５００は、ユーザコンピュータ３００に固有のマシン情報の一例であるＭＡＣアドレスを取得し（Ｓ１０２）、このＭＡＣアドレスを通信ネットワークＣＮを介して、ＤＲＭコンピュータ２００に送信する（Ｓ１０３）。

ＤＲＭコンピュータ２００は、ゲームマネージャ５００から受信したＭＡＣアドレスを、ユーザ情報データベース２４０に登録する（Ｓ１２１，Ｓ１２２）。こ

２５ の時点では、ＭＡＣアドレスのみが判明しているだけであり、ユーザＩＤ等との

対応付けはされない。なお、MAC アドレスをユーザ情報データベース 240 に登録せずに、メモリに保持しておき、ユーザ認証が成功した場合に、ユーザ ID やセッション ID 等と共に MAC アドレスをユーザ情報データベース 240 に登録してもよい。

- 5 DRMコンピュータ 200 は、セッション ID を発行し、また、報告周期を設定する。最初に設定される報告周期には、予め設定された初期値を用いることができる。そして、DRMコンピュータ 200 は、セッション ID と初回の報告周期とをゲームマネージャ 500 に通知する (S123)。

ゲームマネージャ 500 は、セッション ID 及び報告周期を受信すると (S1
10 04)、これらの情報をユーザコンピュータ 300 のメモリに格納して保持する。

次に、ゲームマネージャ 500 は、ユーザからユーザ ID 及びパスワードが入力されたか否かを判定する (S105)。例えば、ユーザがゲームアイコンを選択操作したときに、ユーザ ID 及びパスワードの入力を求める画面を表示させることにより、ユーザにユーザ ID 及びパスワードの入力を促すことができる。

- 15 ゲームマネージャ 500 は、ユーザ ID 及びパスワードの入力を確認すると (S105: YES)、入力されたユーザ ID 及びパスワードと、ユーザが実行を希望するゲームプログラム 400 のゲーム ID とを DRMコンピュータ 200 に送信する (S106)。

DRMコンピュータ 200 は、ゲームマネージャ 500 からユーザ ID、パスワード及びゲーム ID を受信すると (S124)、ユーザ情報データベース 240
20 を参照し、ユーザ認証を行う (S125)。予め登録されているユーザ ID 及びパスワードと、ゲームマネージャ 500 から受信したユーザ ID 及びパスワードとが一致する場合 (S125: YES)、ユーザ認証は成功する。DRMコンピュータ 200 は、ユーザ ID、パスワード、MAC アドレス等を対応付けてユーザ情報データベース 240 に登録する (S127)。逆に、ユーザ ID またはパスワードのい
25

ずれか一方が一致しない場合 (S125: NO)、ユーザ認証は失敗し、エラー処理が行われる (S 1 2 6)。エラー処理としては、例えば、「IDまたはパスワードが違います」等のメッセージをユーザコンピュータ 3 0 0 の画面に表示させることが考えられる。また、例えば、所定回数以上ユーザ認証が失敗した場合は、ゲームプログラム 4 0 0 の起動をロックさせることも可能である。なお、ユーザ認証の情報としては、ユーザ ID 及びパスワードに限らず、例えば、声紋、指紋、虹彩等の生体情報を採用してもよい。

DRMコンピュータ 2 0 0 は、ユーザ認証の成功によって、ユーザが希望するゲームプログラム 4 0 0 の実行許可を決定する (S 1 2 8)。DRMコンピュータ 2 0 0 は、実行を許可したゲームプログラム 4 0 0 をゲームマネージャ 5 0 0 が起動できるようにするための情報を生成して暗号化する (S 1 2 9)。このゲーム起動用の情報としては、例えば、ファイル名等の実行情報やアクティベートキー等を挙げることができる。DRMコンピュータ 2 0 0 は、これら実行情報及びアクティベートキーを、例えば、セッション ID やユーザ情報 (MAC アドレス等) を用いて暗号化し、この暗号化された情報をゲームマネージャ 5 0 0 に送信する (S 1 3 0)。

ゲームマネージャ 5 0 0 は、DRMコンピュータ 2 0 0 から暗号化情報を受信すると (S 1 0 7)、暗号化情報を解凍して (S 1 0 8)、アクティベートキー及び実行情報を取得する (S 1 0 9)。DRMコンピュータ 2 0 0 が使用する暗号アルゴリズムは、ゲームマネージャ 5 0 0 にとって既知であり、解凍に必要な情報はユーザコンピュータ 3 0 0 側にも存在するので、暗号化情報を解凍することができる。

ゲームマネージャ 5 0 0 は、入手したアクティベートキーによってゲームプログラム 4 0 0 をデコードし、このデコードしたゲームプログラム 4 0 0 をユーザコンピュータ 3 0 0 のメモリに格納させる (S 1 1 0)。

即ち、記録媒体RMを用いてゲームプログラム400をユーザコンピュータ300にインストールした場合、ゲームプログラムは、例えば、ユーザコンピュータ300の補助記憶装置にエンコードされた状態で記憶される。このエンコードされた状態では、ゲームプログラム400を起動させることはできない。ゲームマネージャ500がDRMコンピュータ200からアクティベートキーを取得してゲームプログラム400をデコードし、ユーザコンピュータ300のメモリに置いた時点で、ゲームプログラム400は起動可能となる。ここで、注意すべき点は、デコードされたゲームプログラム400（実行体プログラム）は、ファイルとして保存されるのではなく、メモリ内にのみ存在する点である。ゲームプログラム400の終了時には、メモリ内のプログラムが消去されるため、再度ゲームをプレイをする場合は、ゲームマネージャ500を介して再びユーザ認証やアクティベートキーの取得等を行う必要がある。

そして、ゲームマネージャ500は、実行情報に基づいて、ユーザコンピュータ300のメモリに置かれたゲームプログラム400を起動させる（S111）。これにより、ユーザは、ゲームプログラム400を実行させて遊ぶことができるようになる。また、ゲームマネージャ500は、ゲームプログラム400の起動と同時に（物理的に厳密な意味で同時でなくてもよい）、監視プログラム600を起動させる（S112）。監視プログラム600の動作については、さらに後述する。

次に、ゲームプログラム400の実行継続を制御するための監視処理について、図10に基づき説明する。

ゲームマネージャ500は、起動時にDRMコンピュータ200から設定された報告周期を参照する（S141）。ゲームマネージャ500は、ユーザコンピュータ300が有するタイマ機能等を利用することにより、DRMコンピュータ200から予め設定された報告時期が到来したか否かを判定する（S142）。

報告時期が到来した場合 (S142: YES)、ゲームマネージャ 500 は、DRM コンピュータ 200 から設定されたセッション ID をユーザコンピュータ 300 のメモリから読出し (S143)、この読み出したセッション ID を DRM コンピュータ 200 に送信する (S144)。

- 5 DRM コンピュータ 200 は、ゲームマネージャ 500 からセッション ID を受信すると (S161)、ユーザ情報データベース 240 を参照する。DRM コンピュータ 200 は、ユーザ情報データベース 240 に登録されている発行済セッション ID と、ゲームマネージャ 500 から受信したセッション ID とを比較し、両者が一致するか否かを判定する (S163)。なお、ゲームマネージャ 500 から DRM コンピュータ 200 に対して、セッション ID のみを送信してもよいし、
10 あるいは、セッション ID に加えて、例えば、ユーザ ID 等のユーザ情報の全部または一部を含めることもできる。さらには、ユーザコンピュータ 300 の環境情報 (CPU 利用率やメモリ消費量等) を含めることも可能である。しかし、セッション ID に付加する情報が増大するほど、ユーザコンピュータ 300 の負荷
15 は増し、また、ネットワークトラフィックも増大する。

ゲームマネージャ 500 から受信したセッション ID が予め登録されているセッション ID と一致しない場合 (S163: NO)、DRM コンピュータ 200 (継続実行管理部 230) は、ゲームマネージャ 500 に対して、ゲームプログラム 400 の実行継続の禁止を通知する (S164)。両セッション ID が不一致の場合
20 は、別のユーザコンピュータでゲームプログラム 400 を実行等している場合、即ち、例えば、1 つのユーザ ID で同一のゲームプログラム 400 を複数起動しているような場合である。そこで、両セッション ID が不一致の場合は、ゲームプログラム 400 の強制終了をゲームマネージャ 500 に指令する。

ゲームマネージャ 500 から受信したセッション ID と予め登録されているセッション ID とが一致する場合 (S163: YES)、DRM コンピュータ 200 は、新
25 ュ

たな報告周期、即ち、次回の報告時期を算出する（S 1 6 5）。この新たな報告周期の算出については、さらに後述するが、DRMコンピュータ 2 0 0 の負荷状態等を考慮して決定される。

両セッションIDが一致する場合、DRMコンピュータ 2 0 0 は、新たに算出された報告周期と実行継続の許可とをゲームマネージャ 5 0 0 に通知する（S 1 6 6）。

ゲームマネージャ 5 0 0 は、DRMコンピュータ 2 0 0 から実行継続の可否について応答を受信する（S 1 4 5）。ゲームマネージャ 5 0 0 は、ゲームプログラム 4 0 0 の実行継続が許可された場合（S146: YES）、新たに設定された報告周期をユーザコンピュータ 3 0 0 のメモリに保存して、S 1 4 1 に戻り、報告時期の到来を待つ。

逆に、DRMコンピュータ 2 0 0 から実行継続が禁止された場合（S146: NO）、ゲームマネージャ 5 0 0 は、実行中のゲームプログラム 4 0 0 を強制的に終了させる（S 1 4 7）。そして、ゲームマネージャ 5 0 0 は、監視プログラム 6 0 0 を終了させた後（S 1 4 8）、自身も終了させる（S 1 4 9）。

上述のように、ゲームマネージャ 5 0 0 は、DRMコンピュータ 2 0 0 との間で簡易な認証を定期的に行う。これにより、例えば、同一のユーザID及びパスワードを用いてゲームプログラム 4 0 0 を複数起動させるような不正な利用を防止することができる。

図 1 1 は、報告周期の設定処理を示すフローチャートである。図 1 0 中の S 1 6 5 の内容を具体化した一例である。DRMコンピュータ 3 0 0 （詳しくは、継続実行管理部 2 3 0）は、ゲームマネージャ 5 0 0 からセッションIDを受信した時刻を参照する（S 1 8 1）。次に、ゲームマネージャ 5 0 0 は、このセッションIDの受信に関連付けられていた報告周期を参照する（S 1 8 2）。

ゲームマネージャ 5 0 0 は、セッションIDの受信時刻と予め設定されていた

報告周期とのずれを算出する。例えば、セッションIDの受信予定時刻よりも実際の受信時刻が遅れている場合は、通信ネットワークCNの混雑によるパケット到着の遅れや、DRMコンピュータ300の負荷増大による応答性能の低下等を原因として挙げることができる。

- 5 DRMコンピュータ200は、自身の現在の負荷状態を検出する(S184)。
この負荷状態としては、例えば、現在プレイ中のユーザ数、即ち、オンラインによる定期的な認証処理を行うべきゲームマネージャ数を挙げることができる。これに加えて、例えば、CPU利用率、メモリ消費量、データ入出力処理速度(I/O速度)等を検出してもよい。
- 10 DRMコンピュータ200は、現在の負荷状態に基づいて、将来の負荷状態を予測する(S185)。即ち、DRMコンピュータ200は、ゲームマネージャ500の報告周期を現在値に維持した場合に、次の報告時期におけるDRMコンピュータ200の負荷状態を予測する。具体的には例えば、もしも仮に、現在の報告周期が「1時間」に設定されている場合、現在時刻から1時間後にオンライン
- 15 認証を行うユーザ数(ゲームマネージャ数)は、監視状況データベース260により把握できる。

次に、DRMコンピュータ200は、実行中のゲームプログラム400に予め設定されている報告モードを参照する(S186)。ゲームプログラム400に関連付けられる報告モードは、記録媒体RMの流通後でも変更可能である。例えば、

20 サプライヤコンピュータ100からDRMコンピュータ200に対して、ゲームID及び新たな報告モードを通知し、ゲーム情報データベース250の更新を要求すればよい。

最後に、DRMコンピュータ200は、例えば、報告モードと、セッションIDの受信予定時刻と実際の受信時刻との時間的なずれ量と、将来の予測負荷状態

25 とに基づいて、監視効率が最大となるように、新たな報告周期を算出する(S1

87)。

例えば、新作の人気ゲームプログラムが発売された当初は、そのゲームプログラムのユーザ数が急激に増大する。従って、オンラインによる周期的な簡易認証を行うDRMコンピュータ200の負荷は増大する。報告周期を短く設定するほど、不正使用に対するセキュリティ性が向上するが、その反面、DRMコンピュータ200の負荷も増大する。セキュリティ性を重視するあまりに報告周期を短く設定すると、DRMコンピュータ200の応答性が低下したり、機能停止を招く可能性がある。そこで、新作人気ゲームの発売当初等のように、一時的に負荷が増大するような場合は、報告周期が長くなるように制御する。

10 このように、DRMコンピュータ200は、例えば、監視優先モードの場合、機能停止を招かない範囲で最大限のセキュリティ性が得られるように、報告周期(監視タイミング)を設定することができる。一方、負荷軽減モードの場合、DRMコンピュータ200は、最低限のセキュリティ性を維持できる程度に報告周期を設定することができる。

15 以上は一例であって、負荷状態の予測や報告周期の設定等には、種々のアルゴリズムを取り入れることができる。

次に、図12は、ゲームマネージャ500及び監視プログラム600による相互監視の処理を示すフローチャートである。本実施例では、ゲームマネージャ500と監視プログラム600とは、それぞれ共通の監視対象としてゲームプログラム400の動作状態を監視するほか、お互いも監視対象として定期的に監視している。DRMコンピュータ200とゲームマネージャ500との間の定期的なオンライン認証を外部からの監視とすれば、ゲームマネージャ500及び監視プログラム600による相互監視を内部での監視と位置づけることができる。

ゲームマネージャ500の監視処理について先に説明すると、ゲームマネージャ500は、予め設定された監視時期が到来したか否かを判定する(S201)。

監視時期は比較的短周期に設定するのが好ましい。監視時期が到来すると (S201 : YES)、ゲームマネージャ 500 は、監視プログラム 600 の動作状態を確認し (S203)、監視プログラム 600 が正常に動作しているか否かを判定する (S203)。

5 監視プログラム 600 が正常に動作している場合 (S203 : YES)、次に、ゲームマネージャ 500 は、ゲームプログラム 400 の動作状態を確認し (S204)、ゲームプログラム 400 が正常に動作しているか否かを判定する (S205)。ゲームプログラム 400 も正常に動作している場合 (S205 : YES)、ゲームマネージャ 500 は、次の監視時期が到来するまで待機する (S201)。

10 一方、監視プログラム 600 が動作を停止していた場合 (S203 : NO)、あるいは、ゲームプログラム 400 が動作を停止していた場合 (S205 : NO)、ゲームマネージャ 500 は、強制停止処理 (S206 ~ S208) に移行する。

即ち、ゲームマネージャ 500 は、ゲームプログラム 400 及び監視プログラム 600 の両方の動作を停止させた後 (S206, S207)、ゲームマネージャ 15 自身も停止させる (S208)。ゲームプログラム 400 の動作が停止された場合は、デコードされたゲームプログラム 400 は、ユーザコンピュータ 300 のメモリから直ちに消去ないし破壊される。

なお、既に停止しているプログラムについては、改めて停止を命令する必要はない。例えば、ゲームプログラム 400 の動作停止が確認されて強制停止処理に 20 移行した場合は、ゲームプログラム 400 の動作停止を改めて指示する必要はない。同様に、監視プログラム 600 の動作停止が確認されて強制停止処理に移行した場合は、監視プログラム 600 の動作停止を改めて指示する必要はない。しかし、念のために、ゲームプログラム 400 及び監視プログラム 600 の両方に動作停止を命じてよい。

25 監視プログラム 600 の処理も同様である。監視プログラム 600 は、監視時

期が到来すると (S221: YES)、ゲームマネージャ 500 及びゲームプログラム 400 の動作状態をそれぞれ監視し (S222~S225)、いずれか一方が動作を停止していた場合は (S223: NO、または S225: NO)、強制停止処理に移行し、全てのプログラムを停止させる (S226~S228)。

5. このように、ゲームマネージャ 500 及び監視プログラム 600 という複数の動作監視用プログラムが、ゲームプログラム 400 の動作状態を監視すると共に、それぞれお互いをも監視するため、ゲームプログラム 400 の動作停止をより確実に検出することができる。また、一方の動作監視用プログラムが意図的に停止された場合でも、他方の監視用プログラムが全体のシャットダウンを行うため、
- 10 ユーザコンピュータ 300 のメモリに展開されたゲームプログラム 400 が不正にコピーされるのを未然に防止することができる。

以上詳述した通り、本実施例によれば、ゲームプログラム 400 の作動を制御するゲームマネージャ 500 とライセンス認証を行う DRM コンピュータ 200 との間で、定期的なオンライン認証を行うため、不正使用に対する耐久性を高め

15 ることができる。

また、この定期的なオンライン認証は、セッション ID の比較により行われるため、比較的簡易な処理で済む。従って、コンピュータ負荷を増大させずに、簡易な認証を比較的短周期で行うことができ、長時間にわたってセキュリティ性を維持することも可能となる。

- 20 さらに、オンラインによる簡易認証を行うタイミング (報告周期) を、DRM コンピュータ 200 の負荷状態等に基づいて動的に制御するため、ネットワークトラフィックやコンピュータ負荷等を考慮して、より高いセキュリティ性を実現することができる。

また、ゲームマネージャ 500 及び監視プログラム 600 という、2 種類のそれぞれ独立した動作監視用プログラムを用意し、ゲームプログラム 400 の動作

25

状態のみならず、それぞれお互いの監視をも行い、ゲームプログラム400、ゲームマネージャ500、監視プログラム600のいずれか1つでも動作を停止した場合は、残りの2つのプログラムの動作も停止させ、ゲームプログラム400を消去等して無力化する構成のため、メモリに展開されたゲームプログラム4050を不正に読み出してコピー等する行為を阻止して、信頼性をより高めることができる。

次に、図13は、本発明のさらに別の実施例を示す。本実施例は、第1実施例において、複数の監視用プログラムによる相互監視と、認証用コンピュータとの10間の定期的なオンライン認証とを実現させるものである。

本実施例では、配信用コンピュータ10からユーザコンピュータ30に向けて、ゲームプログラム40と実行制御プログラム50Aと監視プログラム60とが配信される。

実行制御プログラム50Aは、上述した実行制御プログラム50の構成及び作15用に加えて、上述したゲームマネージャ500が実行する定期的な簡易オンライン認証機能と監視機能とを備えている。また、監視プログラム60は、上述した監視プログラム600と同様の監視機能を備えている。

実行制御プログラム50Aは、最初のユーザ認証によりゲームプログラム40のデコード等を行う。また、実行制御プログラム50Aは、認証用コンピュータ2020に対して定期的にセッションIDを送信することにより、ゲームプログラム40の実行中においてもユーザ認証を行う。実行制御プログラム50Aは、ユーザ認証が成功した場合はゲームプログラム40の継続的な実行を許可し、ユーザ認証が失敗した場合はゲームプログラム40を強制的に終了させる。

また、実行制御プログラム50Aと監視プログラム60とは、共にゲームプログラム40の起動状態を監視していると共に、お互い同士もそれぞれ監視してい25

る。そして、ゲームプログラム40、実行制御プログラム50A、監視プログラム60のうちいずれか1つのプログラムが終了した場合は、実行制御プログラム50Aまたは監視プログラム60がこれを検出し、残りのプログラム及び自分自身を終了させる。

- 5 なお、上述した本発明の各実施例は、本発明の説明のための例示であり、本発明の範囲を実施例にのみ限定する趣旨ではない。当業者は、本発明の要旨を逸脱することなしに、他の様々な態様で本発明を実施できる。

請 求 の 範 囲

1. ユーザコンピュータにインストールされた第1のソフトウェアを第2のソフトウェアに更新させるソフトウェア実行制御システムであって、

- 5 エンコードされた前記第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行制御プログラムを前記ユーザコンピュータに通信ネットワークを介して配信する配信部と、

前記ユーザコンピュータにインストールされた前記実行制御プログラムからの要求によってユーザ認証を行い、正当なユーザであると確認した場合には、前記
10 第2のソフトウェアをデコードして起動させるために必要な所定の情報を前記通信ネットワークを介して前記実行制御プログラムに送信する認証部と、
を備え、

前記第2のソフトウェアは前記実行制御プログラムから渡される起動情報のみで起動可能に構成されており、

- 15 前記実行制御プログラムは、

(1) 前記認証部から受信した前記所定の情報に基づいて前記エンコードされた第2のソフトウェアをデコードして前記第1のソフトウェアに置き換え、

(2) 前記所定の情報に基づいて起動情報を生成することにより、前記第2のソフトウェアを起動させ、

- 20 (3) 前記第2のソフトウェアの実行が終了された場合には、前記第2のソフトウェアを無力化させるように構成されているソフトウェア実行制御システム。

2. 前記実行制御プログラムは、複数種類の第2のソフトウェアに対応可能に構成されており、

- 25 前記認証部が前記実行制御プログラムに送信する前記所定の情報には、起動さ

せる第2のソフトウェアの格納先アドレス情報と起動引数と第2のソフトウェアをデコードするためのデコードキー情報とが含まれている請求項1に記載のソフトウェア実行制御システム。

5 3. 前記実行制御プログラムは、前記ユーザコンピュータに固有のマシン情報と暗号化キー情報とを含む認証用情報を前記認証部に送信し、

前記認証部は、少なくとも前記マシン情報に基づいてユーザ認証を行い、正当なユーザであると確認した場合には、前記所定の情報を前記暗号化キー情報で暗号化して前記通信ネットワークを介して前記実行制御プログラムに送信するもの

10 であり、

かつ、前記認証部には、前記マシン情報を複数個登録可能である請求項1に記載のソフトウェア実行制御システム。

4. 前記認証部は、正当なユーザであると確認した場合には、該ユーザが起動可能な第2のソフトウェアの一覧データを前記ユーザコンピュータに送信し、
15 前記一覧データから選択された第2のソフトウェアに関する前記所定の情報を前記通信ネットワークを介して前記実行制御プログラムに送信するものである請求項1に記載のソフトウェア実行制御システム。

20 5. 前記実行制御プログラムは、

前記ユーザコンピュータに固有のマシン情報を取得する機能と、

暗号化キー情報を生成する機能と、

前記認証部にユーザ認証を要求し、少なくとも前記マシン情報及び前記暗号化キー情報を前記認証部に送信する機能と、

25 前記認証部から受信した起動可能な第2のソフトウェアの一覧データからいず

れか1つの第2のソフトウェアをユーザに選択させ、選択された第2のソフトウェアを前記認証部に通知する機能と、

前記選択された第2のソフトウェアの前記ユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを少なくとも前記暗号化キー情報5により暗号化してなる所定の情報を受信する機能と、

前記暗号化された所定の情報を少なくとも前記暗号化キー情報により解読する機能と、

前記解読されたデコードキー情報により前記ユーザコンピュータ内の第2のソフトウェアをデコードさせる機能と、

10 前記解読された起動引数及び前記格納先アドレス情報に基づいて、前記起動情報を生成する機能と、

前記生成された起動情報によって前記デコードされた第2のソフトウェアを起動させる機能と、

前記起動された第2のソフトウェアの実行状態を監視し、該第2のソフトウェア15の実行が終了した場合は、前記第2のソフトウェアを無力化させる機能と、

を前記ユーザコンピュータ上に実現させるものである請求項1に記載のソフトウェア実行制御システム。

6. 前記第2のソフトウェアは、プログラムと付随データ群とを含んでなり、

20 前記プログラム又は前記付随データ群の少なくともいずれか一方を更新させるものである請求項1に記載のソフトウェア実行制御システム。

7. 前記ユーザコンピュータにインストールされている前記第1のソフトウェアは、前記第2のソフトウェアに置換されるまでは、前記認証部による認証を

25 受けることなく実行可能である請求項1に記載のソフトウェア実行制御システム。

8. 前記実行制御プログラムは、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアの全部又は一部を削除することにより無力化させるものである請求項1に記載のソフトウェア実行制御システム。

5

9. 前記第2のソフトウェアは、プログラムと付随データ群とを含んでなり、前記実行制御プログラムは、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアのエンコードデータは保存しつつ、前記デコードされた第2のソフトウェアのうち前記プログラムのみを無力化させるものである請求項10 1に記載のソフトウェア実行制御システム。

10. 前記実行制御プログラムは、前記第2のソフトウェアとは別に強制終了させることができないプログラムとして構成されている請求項1に記載のソフトウェア実行制御システム。

15

11. 前記配信部と前記認証部とは、それぞれ別体のコンピュータ上に実現されている請求項1に記載のソフトウェア実行制御システム。

12. 前記実行制御プログラムは、前記第2のソフトウェアの実行中に、前記20 認証部との間で定期的または不定期的ユーザ認証を行うものであり、このユーザ認証が失敗した場合は前記第2のソフトウェアを強制的に終了させる請求項1に記載のソフトウェア実行制御システム。

13. 前記第2のソフトウェアの実行中に行われる定期的または不定期的ユーザ25 認証は、少なくとも予測される将来の認証用コンピュータの負荷状態を考慮し

て、可変に制御可能である請求項 1 2 に記載のソフトウェア実行制御システム。

1 4. 前記配信部は、前記第 2 のソフトウェア及び前記実行制御プログラムと共に監視プログラムを前記ユーザコンピュータに配信し、

5 前記監視プログラムは、前記第 2 のソフトウェア及び前記実行制御プログラムの動作状態をそれぞれ監視し、前記第 2 のソフトウェアまたは前記実行制御プログラムのいずれか一方が動作を停止した場合は、前記第 2 のソフトウェア及び前記実行制御プログラムをそれぞれ停止させ、自身も停止させるものであり、

前記実行制御プログラムは、前記第 2 のソフトウェア及び前記監視プログラム
10 の動作状態をそれぞれ監視し、前記第 2 のソフトウェアまたは前記監視プログラムのいずれか一方が動作を停止した場合は、前記第 2 のソフトウェア及び前記監視プログラムをそれぞれ停止させ、自身も停止させるものである請求項 1 に記載のソフトウェア実行制御システム。

15 1 5. ユーザコンピュータにインストールされた第 1 のソフトウェアを第 2 のソフトウェアに更新し、この第 2 のソフトウェアの実行を制御する実行制御プログラムであって、

外部の認証部と通信ネットワークを介して通信し、ユーザ認証を求める第 1 の機能と、

20 前記認証部から受信した所定の情報に基づいて、前記第 2 のソフトウェアを起動させるための起動情報を生成する第 2 の機能と、

前記認証部から受信した所定の情報に基づいて、前記第 2 のソフトウェアをデコードさせる第 3 の機能と、

前記ユーザコンピュータに既にインストールされている更新前のソフトウェア
25 を前記デコードされた第 2 のソフトウェアに置き換える第 4 の機能と、

前記生成された起動情報によって前記第 2 のソフトウェアを起動させる第 5 の機能と、

前記第 2 のソフトウェアの実行状態を監視し、前記第 2 のソフトウェアの実行が終了した場合は、前記第 2 のソフトウェアを無能力化させる第 6 の機能と、

5 を前記ユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

16. 前記第 2 のソフトウェアは、プログラムと付随データ群とを含んでなり、

前記第 4 の機能は、前記プログラム又は前記付随データ群の少なくともいずれ
10 か一方を置き換えるものである請求項 15 に記載のソフトウェアの実行制御プログラム。

17. 前記ユーザコンピュータに既にインストールされている更新前のソフトウェアは、前記第 4 の機能によって前記第 2 のソフトウェアに置換される前は、
15 前記認証部による認証を受けることなく実行可能である請求項 16 に記載のソフトウェアの実行制御プログラム。

18. 前記第 6 の機能は、前記第 2 のソフトウェアの実行が終了した場合は、前記第 2 のソフトウェアの全部又は一部を削除することにより無能力化させるもの
20 である請求項 17 に記載のソフトウェアの実行制御プログラム。

19. 前記第 2 のソフトウェアは、プログラムと付随データ群とを含んでなり、

前記第 6 の機能は、前記第 2 のソフトウェアの実行が終了した場合は、前記第
25 2 のソフトウェアのエンコードデータは保存しつつ、前記デコードされた第 2 の

ソフトウェアのうち前記プログラムのみを無力化させるものである請求項 17 に記載のソフトウェアの実行制御プログラム。

20. 前記実行制御プログラムは、前記第 2 のソフトウェアとは別に強制終了させることができないプログラムとして構成されている請求項 15 に記載のソフトウェアの実行制御プログラム。

21. ユーザコンピュータにインストールされたソフトウェアを第 2 のソフトウェアに更新し、この第 2 のソフトウェアの実行を制御する実行制御プログラムであって、

前記ユーザコンピュータに固有のマシン情報を取得する機能と、

暗号化キー情報を生成する機能と、

外部の認証部にユーザ認証を要求し、少なくとも前記マシン情報及び前記暗号化キー情報を前記認証部に送信する機能と、

15 前記認証部から受信した起動可能な第 2 のソフトウェアの一覧データからいずれか 1 つの第 2 のソフトウェアをユーザに選択させ、選択された第 2 のソフトウェアを前記認証部に通知する機能と、

前記選択された第 2 のソフトウェアの前記ユーザコンピュータにおける格納先アドレス情報と起動引数とデコードキー情報とを前記暗号化キー情報により暗号

20 化してなる所定の情報を受信する機能と、

前記暗号化された所定の情報を少なくとも前記暗号化キー情報により解読する機能と、

前記解読されたデコードキー情報により前記ユーザコンピュータ内の第 2 のソフトウェアをデコードさせる機能と、

25 前記解読された起動引数及び前記格納先アドレス情報に基づいて、前記起動情

報を生成する機能と、

前記生成された起動情報によって前記デコードされた第2のソフトウェアを起動させる機能と、

前記起動された第2のソフトウェアの実行状態を監視し、該第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアを無効化させる機能と、
5 前記ユーザコンピュータ上に実現させるソフトウェアの実行制御プログラム。

22. ユーザコンピュータにインストールされている自由に使用可能な第1のソフトウェアを第2のソフトウェアに更新可能である旨をユーザに通知させる
10 ステップと、

前記第2のソフトウェアを配信する配信用コンピュータに前記ユーザコンピュータを通信ネットワークを介して接続させ、前記第2のソフトウェアへの更新を要求させるステップと、

前記配信用コンピュータから前記ユーザコンピュータにエンコードされた前記
15 第2のソフトウェア及び該第2のソフトウェアの実行を制御するための実行制御プログラムを通信ネットワークを介して送信させるステップと、

前記ユーザコンピュータ上で起動した前記実行制御プログラムにより、前記ユーザコンピュータと認証用コンピュータとを通信ネットワークを介して接続させ、前記認証用コンピュータにユーザ認証を要求させるステップと、

20 前記ユーザ認証により正当なユーザであると認められた場合に前記認証用コンピュータから前記ユーザコンピュータに送信される所定の情報に基づいて、前記第2のソフトウェアをデコードするステップと、

前記認証用コンピュータから受信した前記所定の情報に基づいて、前記第2のソフトウェアを起動させるための起動情報を生成させるステップと、

25 前記生成された起動情報によって前記第2のソフトウェアを起動させるステッ

ブと、

前記起動された第2のソフトウェアの実行を監視し、前記第2のソフトウェアの実行が終了した場合は、前記第2のソフトウェアを無効化させるステップと、
を含んでなるソフトウェアの更新方法。

5

23. 第1のソフトウェアに置換される第2のソフトウェアと共にユーザコンピュータにインストールされる実行制御プログラムからの要求によってユーザ認証を行う認証部と、

前記認証部により正当なユーザであると確認された場合は、前記第2のソフトウェアをデコードして起動させるために必要な所定の情報を前記実行制御プログラムに送信する情報送信部と、

を備え、

前記第2のソフトウェアは前記実行制御プログラムから渡される起動情報のみで起動可能に構成されており、

15 前記実行制御プログラムは、

(1) 前記認証部から受信した前記所定の情報に基づいて前記エンコードされた第2のソフトウェアをデコードして前記第1のソフトウェアに置き換え、

(2) 前記所定の情報に基づいて起動情報を生成することにより、前記第2のソフトウェアを起動させ、

20 (3) 前記第2のソフトウェアの実行が終了された場合には、前記第2のソフトウェアを無効化させるように構成されているコンピュータ。

24. アプリケーションソフトウェア及び監視プログラムと共にユーザコンピュータにインストールされる実行制御プログラムと通信を行うことにより、前記実行制御プログラムの動作を制御する管理用コンピュータであって、

25

前記実行制御プログラムからの要求に基づいてユーザ認証を行う認証部と、

前記認証部により正当なユーザであると確認された場合は、前記実行制御プログラムが前記アプリケーションソフトウェアを起動させるために必要な第 1 の情報を前記実行制御プログラムに送信する情報送信部と、

- 5 所定の時期に前記実行制御プログラムとの間で行われる継続確認通信に基づいて、前記アプリケーションソフトウェアの実行継続を許可するか否かを管理する継続実行管理部と、を備えた管理用コンピュータ。

25. 前記継続実行管理部は、前記継続確認通信によって前記実行制御プログラムから取得される第 1 の識別情報と前記ユーザ認証に予め関連付けられている第 2 の識別情報とを比較し、両方の識別情報が対応する場合は、前記実行制御プログラムに対して前記アプリケーションソフトウェアの実行継続を許可し、前記各識別情報が対応していない場合は、前記実行制御プログラムに対して前記アプリケーションソフトウェアの実行継続を禁止させる請求項 24 に記載の管理用コンピュータ。

26. 前記継続実行管理部は、前記第 2 の識別情報に対応する前記第 1 の識別情報を予め前記実行制御プログラムに設定させる請求項 25 に記載の管理用コンピュータ。

27. 前記継続実行管理部は、前記所定の時期を前記実行制御プログラムに予め設定し、この予め設定された所定の時期が到来した場合は、前記実行制御プログラムから前記継続実行管理部に対して前記継続確認通信を行わせる請求項 24 に記載の管理用コンピュータ。

28. 前記継続実行管理部は、前記所定の時期を可変に設定可能である請求項24に記載の管理用コンピュータ。

29. 前記継続実行管理部は、少なくとも予測される将来の負荷状態を考慮して、前記所定の時期を可変に設定可能である請求項28に記載の管理用コンピュータ。

30. 前記監視プログラムは、前記アプリケーションソフトウェア及び前記実行制御プログラムの動作状態をそれぞれ監視し、前記アプリケーションソフトウェアまたは前記実行制御プログラムのいずれか一方が動作を停止した場合は、前記アプリケーションソフトウェア及び前記実行制御プログラムをそれぞれ停止させ、自身も停止させるものであり、

前記実行制御プログラムは、前記アプリケーションソフトウェア及び前記監視プログラムの動作状態をそれぞれ監視し、前記アプリケーションソフトウェアまたは前記監視プログラムのいずれか一方が動作を停止した場合は、前記アプリケーションソフトウェア及び前記監視プログラムをそれぞれ停止させ、自身も停止させるものである請求項24に記載の管理用コンピュータ。

31. アプリケーションソフトウェアが実行されるユーザコンピュータと、前記アプリケーションソフトウェアの実行を管理する管理用コンピュータとを備えたソフトウェア実行制御システムであって、

前記ユーザコンピュータには、

前記アプリケーションソフトウェアの実行を制御するための実行制御部と、

前記アプリケーションソフトウェア及び前記実行制御プログラムの動作を監視するための監視部とが設けられ、

前記管理用コンピュータには、

前記実行制御プログラムからの要求に基づいてユーザ認証を行う認証部と、

前記認証部により正当なユーザであると確認された場合は、前記実行制御部が前記アプリケーションソフトウェアを起動させるために必要な第1の情報を前記

5 実行制御部に送信する情報送信部と、

所定の時期に前記実行制御部との間で行われる継続確認通信に基づいて、前記アプリケーションソフトウェアの実行継続を許可するか否かを管理する継続実行管理部とが設けられているソフトウェア実行制御システム。

10 32. コンピュータを、アプリケーションソフトウェアの実行を制御する実行制御部と、前記アプリケーションソフトウェア及び前記実行制御部の動作状態をそれぞれ監視する監視部として、機能させるためのコンピュータプログラムであって、

前記実行制御部は、

15 管理用コンピュータと通信することによりユーザ認証を要求する機能と、

前記管理用コンピュータから受信した第1の情報に基づいて、前記アプリケーションソフトウェアを起動させる機能と、

前記管理用コンピュータとの間で継続確認通信を行う機能と、

前記継続確認通信によって前記アプリケーションソフトウェアの実行継続が禁

20 止された場合は、前記アプリケーションソフトウェアの動作を停止させる機能と、
を備え、

前記監視部は、

前記アプリケーションソフトウェア及び前記実行制御部の動作状態をそれぞれ監視する機能と、

25 前記アプリケーションソフトウェアまたは前記実行制御部のいずれか一方が動

作を停止した場合は、前記アプリケーションソフトウェア及び前記実行制御部をそれぞれ停止させ、自身も停止させる機能と、
を備えているコンピュータプログラム。

5 33. 前記実行制御部は、さらに、

前記アプリケーションソフトウェア及び前記監視部の動作状態をそれぞれ監視する機能と、

前記アプリケーションソフトウェアまたは前記監視部のいずれか一方が動作を停止した場合は、前記アプリケーションソフトウェア及び前記監視部をそれぞれ
10 停止させ、自身も停止させる機能を備えている請求項32に記載のコンピュータプログラム。

34. 前記実行制御部の前記継続確認通信を行う機能は、前記管理用コンピュータから予め設定された所定の時期に、前記管理用コンピュータから予め設定
15 された第1の識別情報を前記管理用コンピュータに送信するものである請求項32に記載のコンピュータプログラム。

35. 前記継続確認通信を行う度に、前記管理用コンピュータから前記所定の時期が可変に設定される請求項34に記載のコンピュータプログラム。

20

36. 前記アプリケーションソフトウェアと、前記実行制御部と、前記監視部とは、同一の記録媒体に記録されて流通するものである請求項32に記載のコンピュータプログラム。

FIG. 1

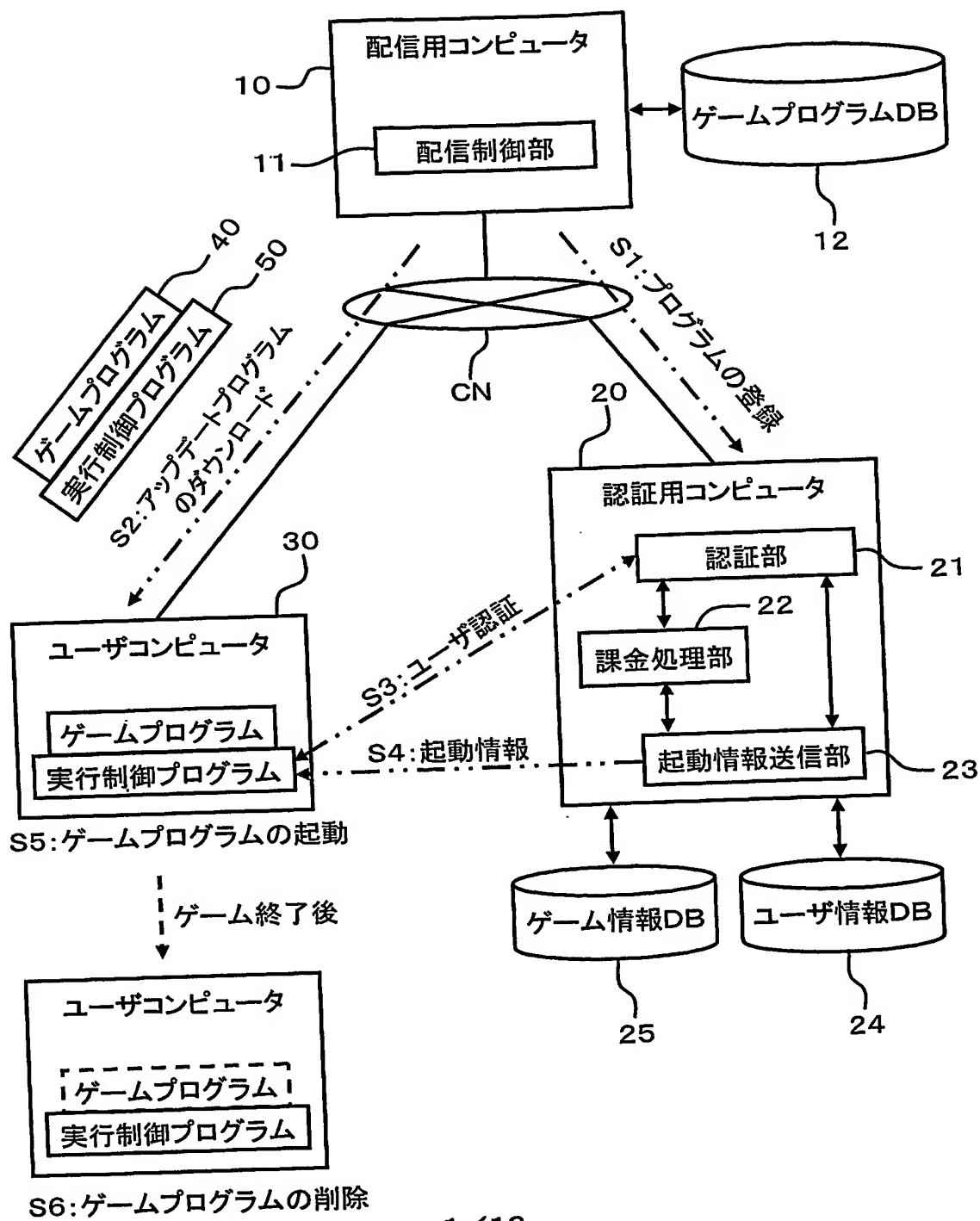


FIG. 2

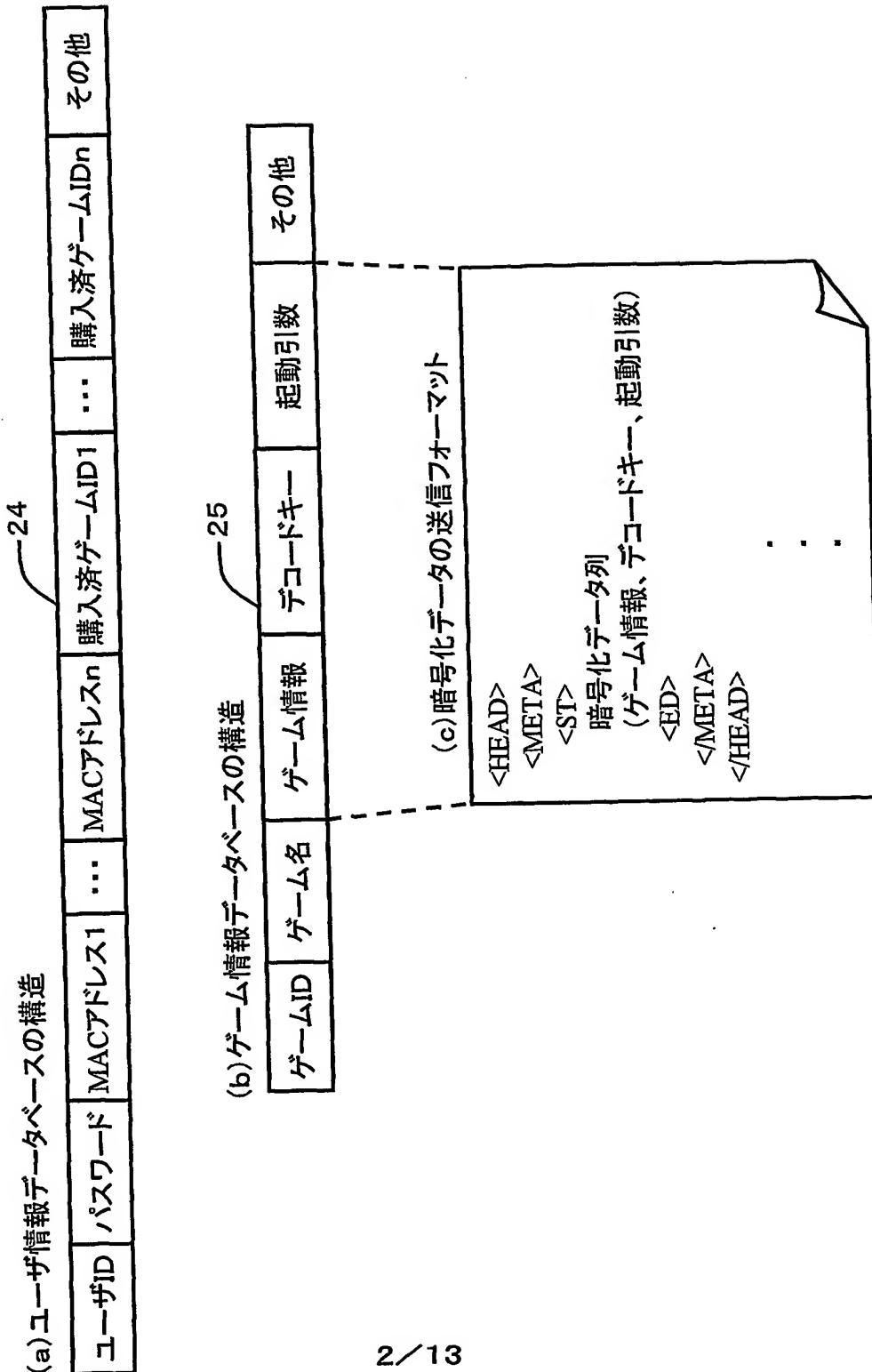
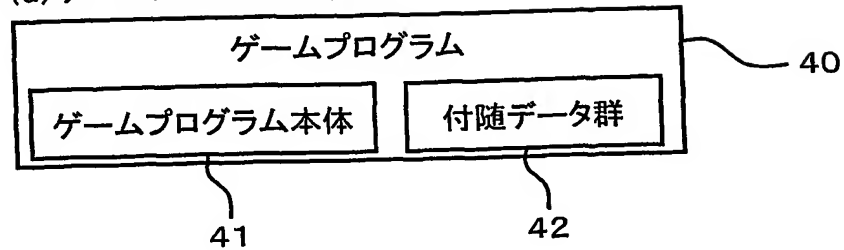


FIG. 3

(a) ゲームプログラムの構造



(b) 実行制御プログラムの構造

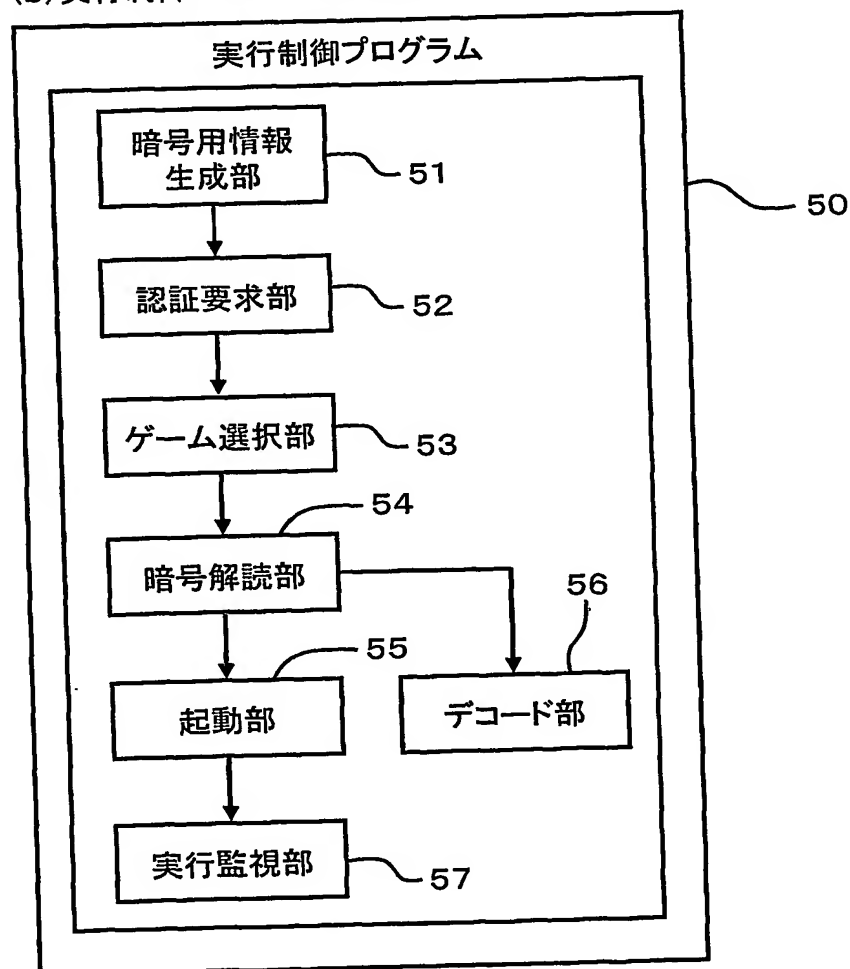


FIG. 4

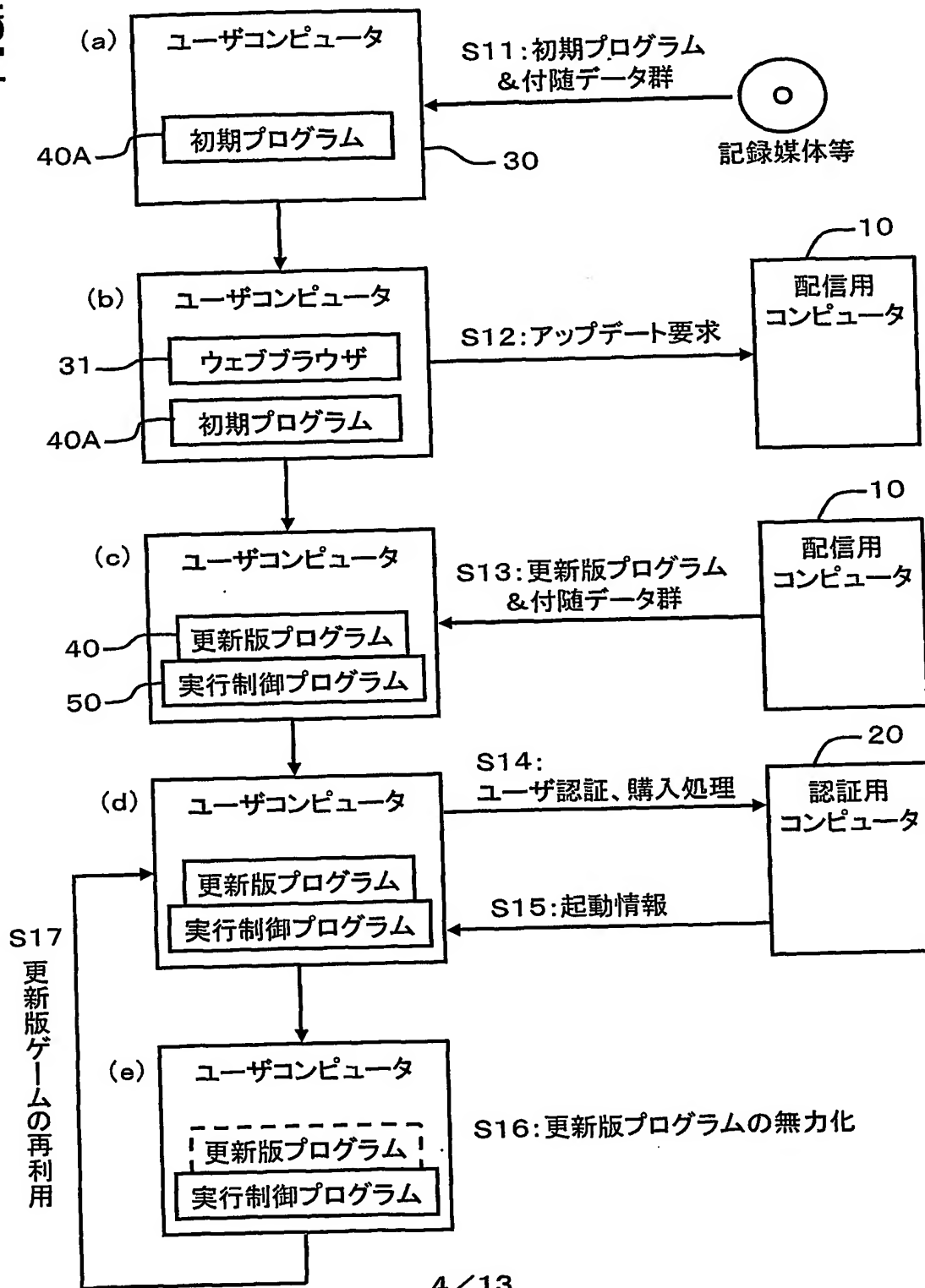


FIG. 5

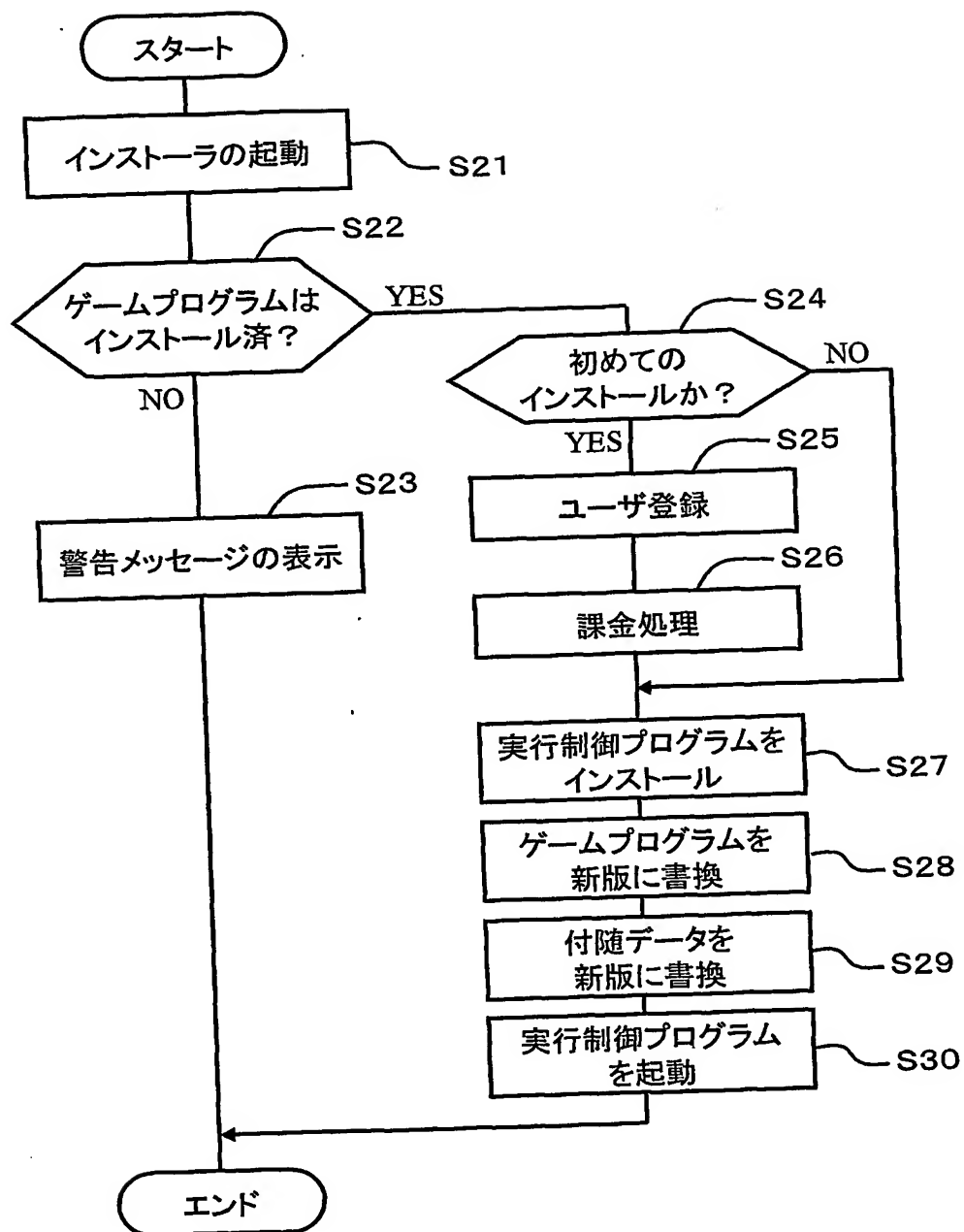


FIG. 6

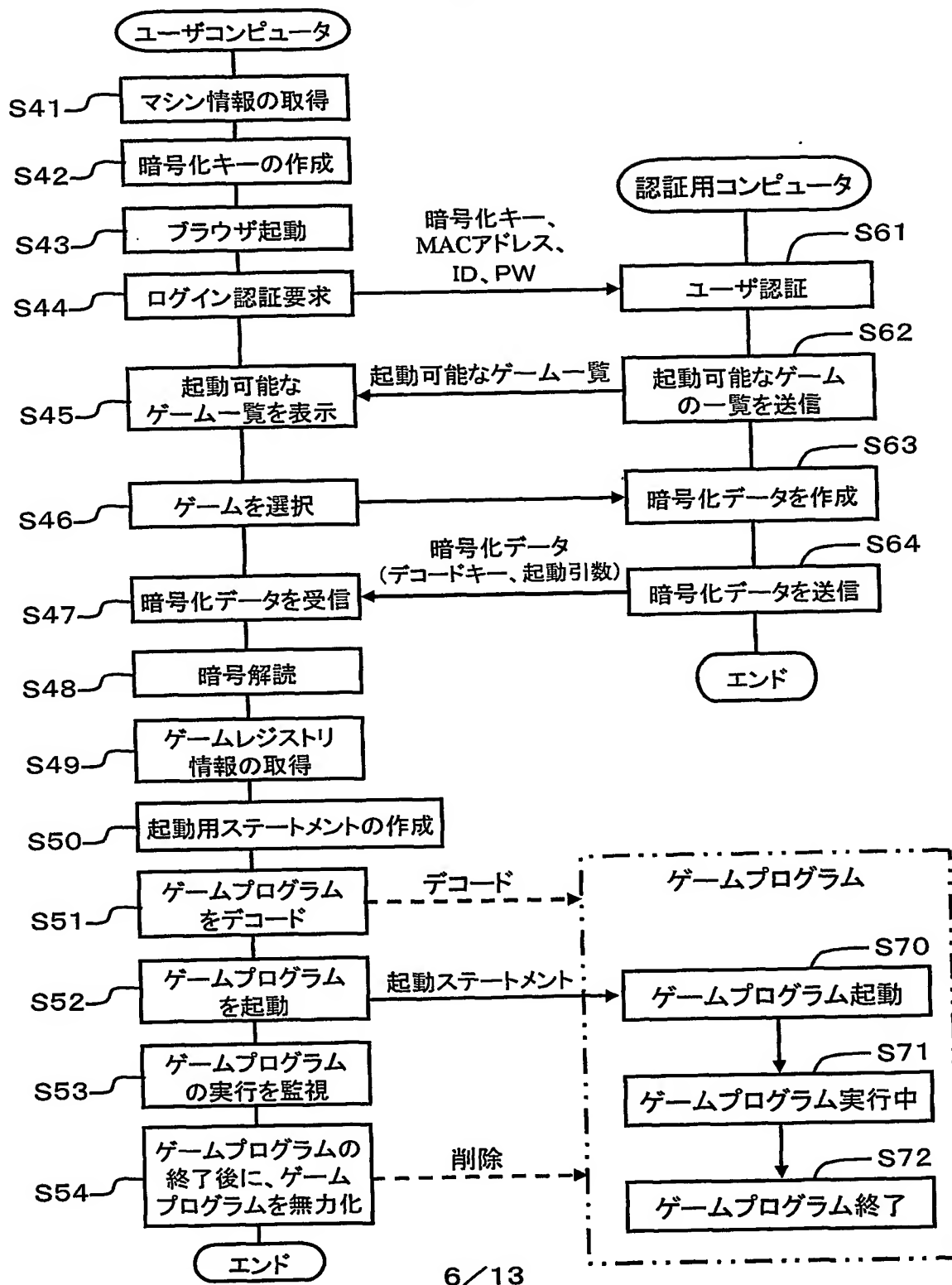


FIG. 7

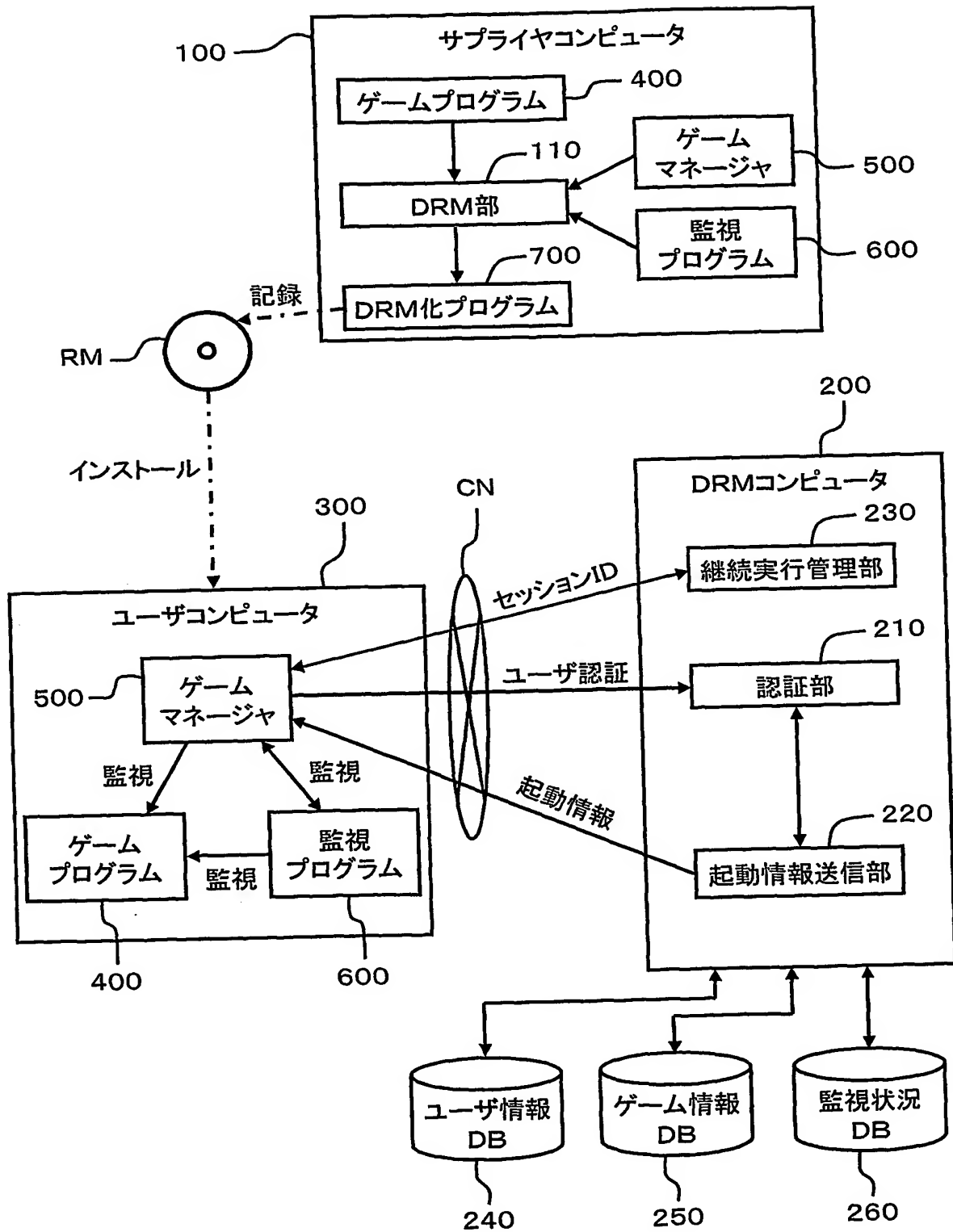


FIG. 8

(a) 240

ユーザ情報データベース				
ユーザID	PW	MACアドレス	セッションID	その他
Interlex	Buddy	00-11-22-33-44-AA	Aaabbbsccdd...	

(b) 250

ゲーム情報データベース					
ゲームID	ゲーム名	ゲーム情報	デコードキー	起動引数	報告モード
					初回のみ
					毎起動時
					監視優先
					負荷軽減

(c) 260

監視状況データベース					
ユーザID	報告周期	予定報告時期	ゲームID	ゲームスタート時刻	その他
ユーザ1	30分間隔	16:25	ゲーム1	13:01	
ユーザ2	40分間隔	16:00	ゲーム2	15:20	
ユーザ3	10分間隔	16:00	ゲーム3	15:30	

FIG. 9

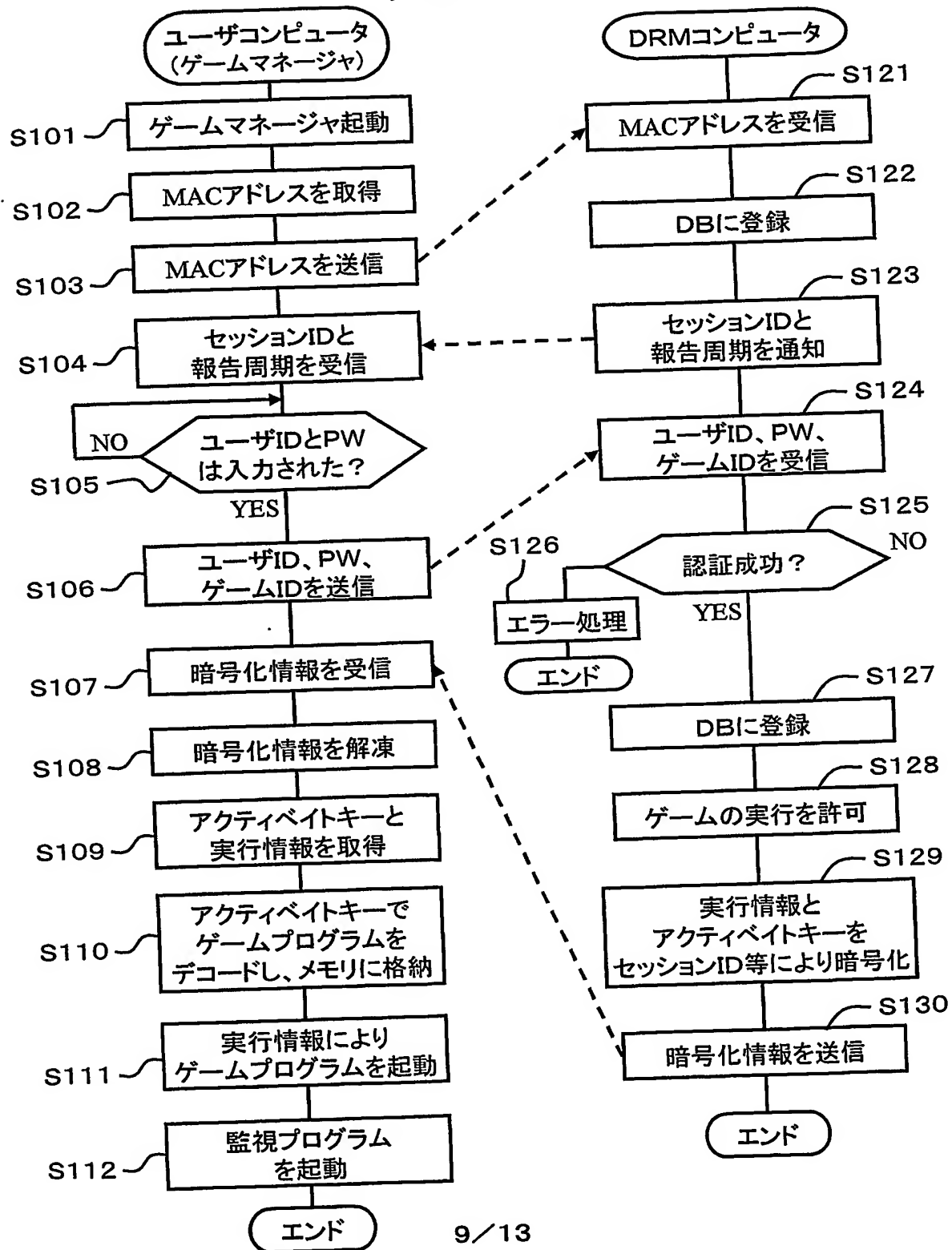


FIG. 10

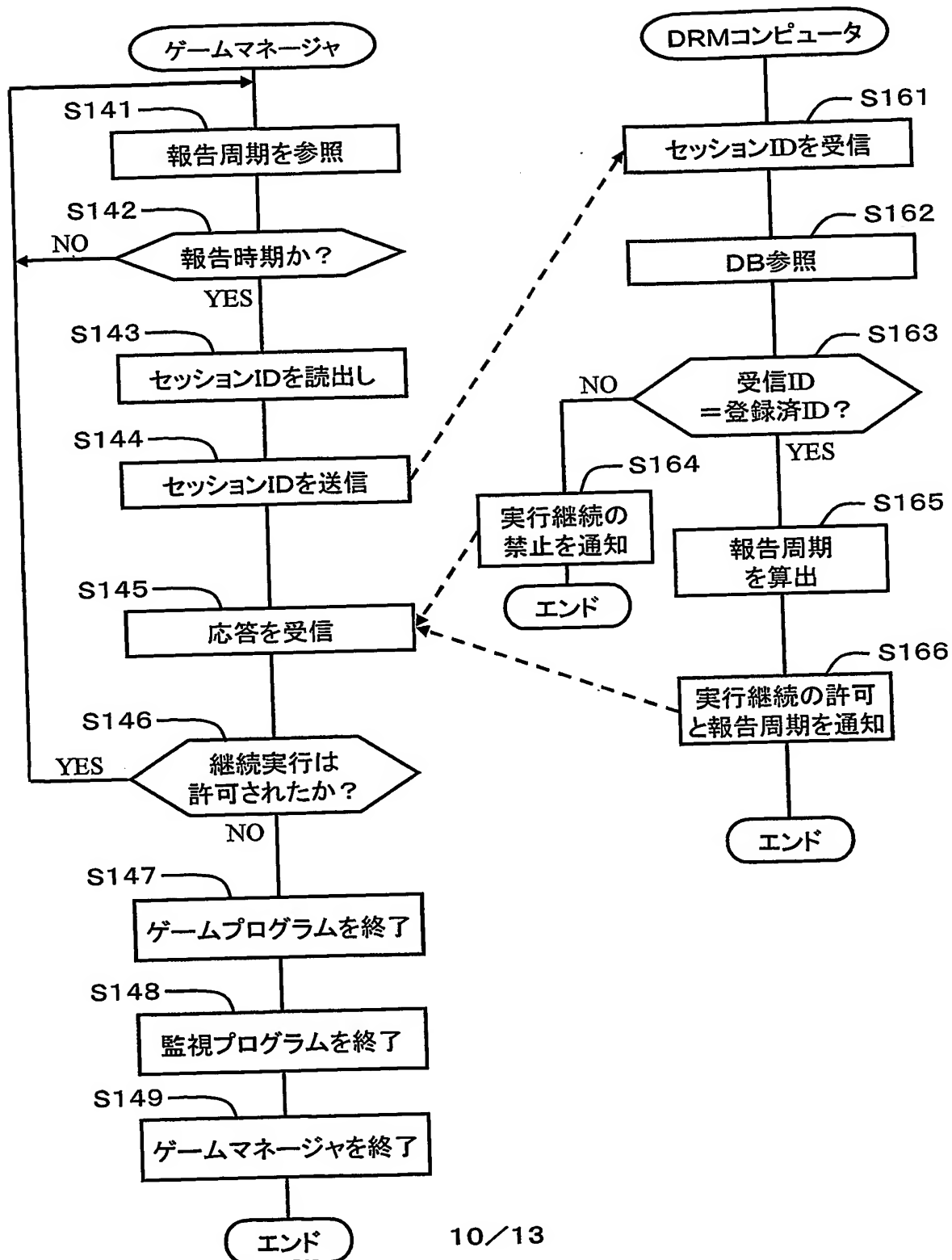


FIG. 11

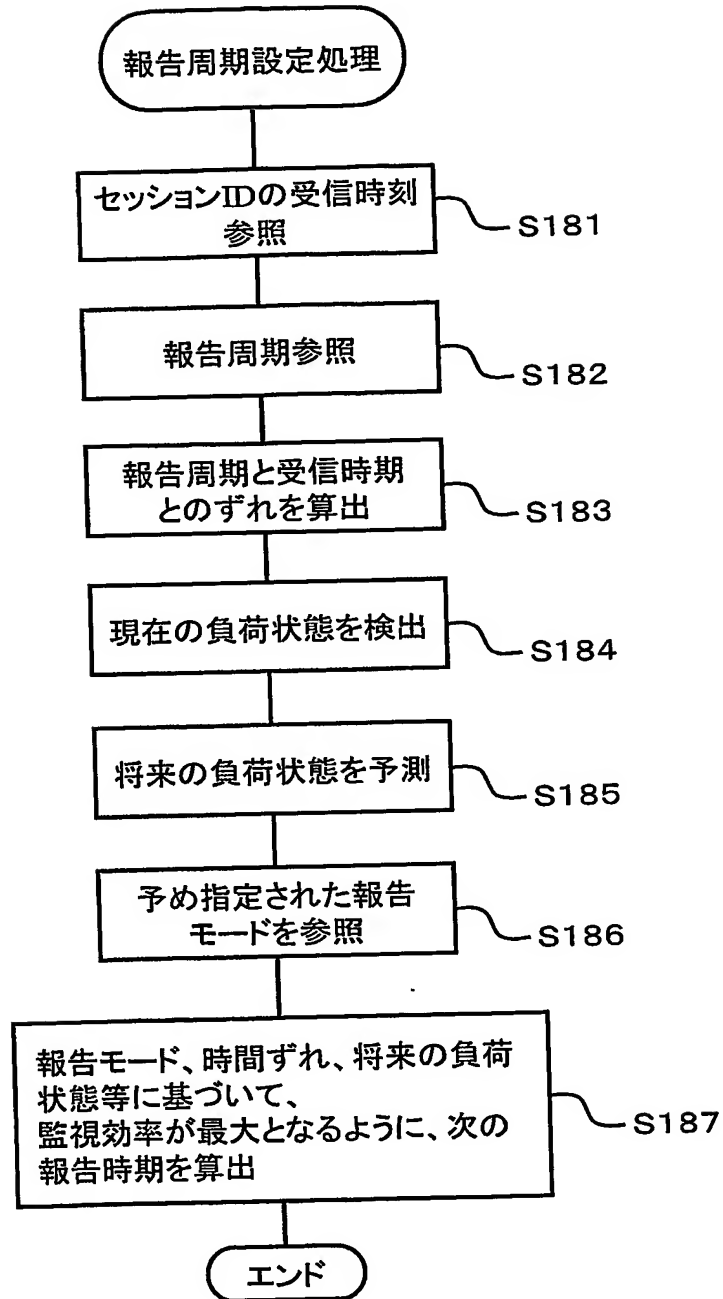


FIG. 12

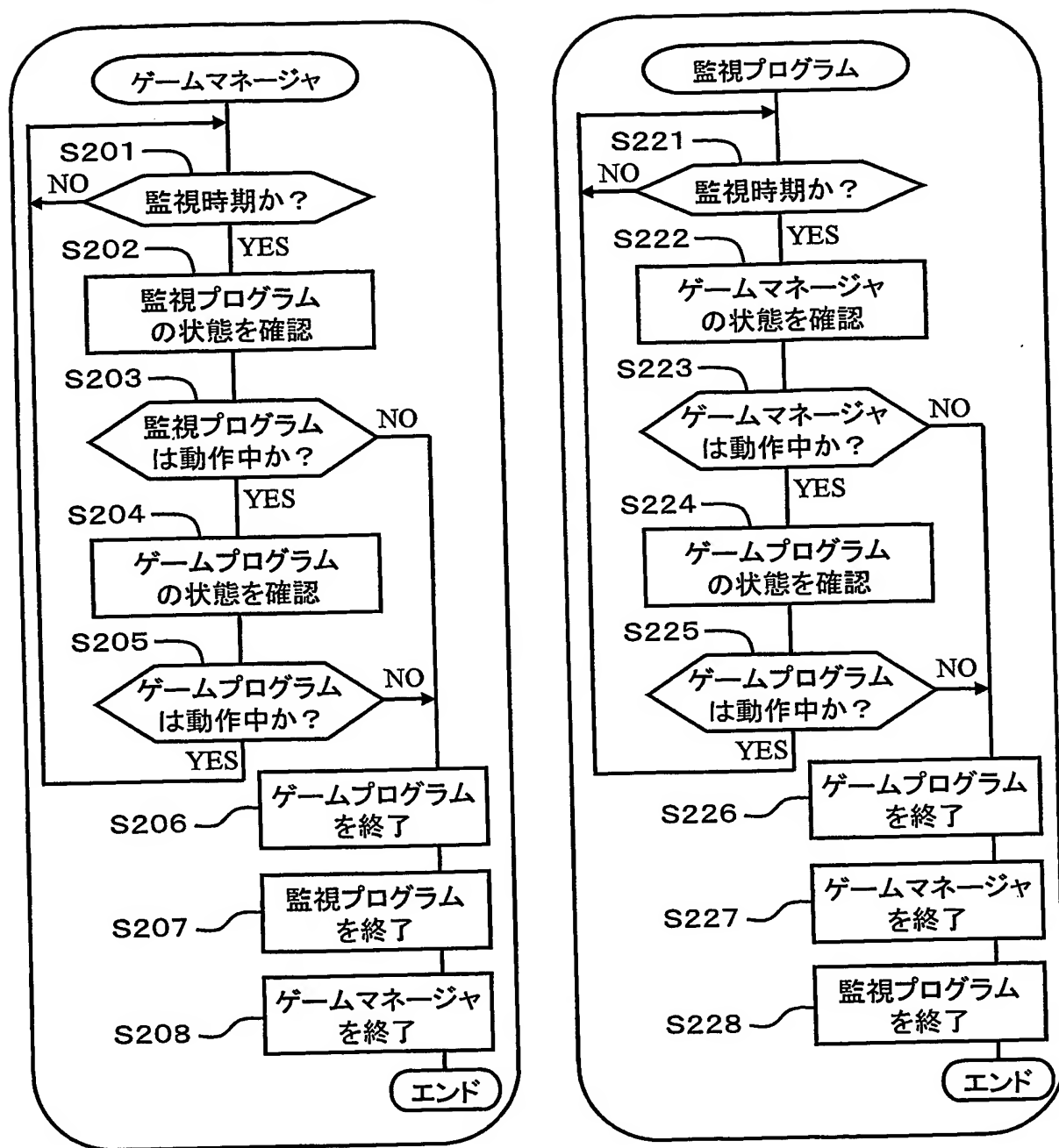
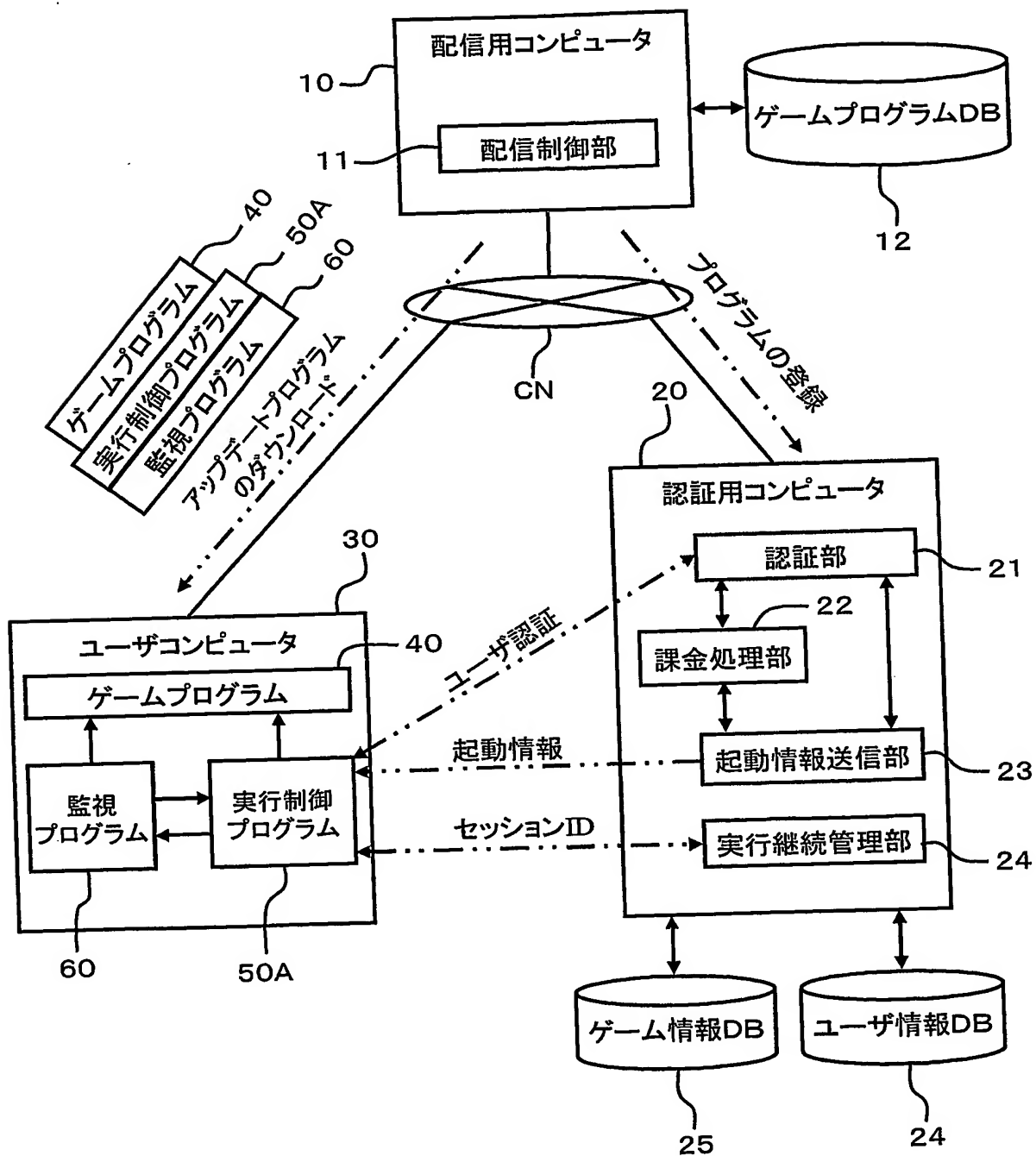


FIG. 13



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/15779

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁷ G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F1/00, 12/14, 15/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-229660 A (Toshiba Corp.), 16 August, 2002 (16.08.02), Full text; Figs. 1 to 5 (Family: none)	1-23
Y	JP 10-133869 A (Shin'ichiro OGAWA), 22 May, 1998 (22.05.98), Full text; Figs. 1 to 2 (Family: none)	1-23
Y	JP 8-6784 A (Nippon Telegraph And Telephone Corp.), 12 January, 1996 (12.01.96), Full text; particularly, Par. No. [0053]; Figs. 1 to 3 (Family: none)	1-23

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
23 February, 2004 (23.02.04)

Date of mailing of the international search report
02 March, 2004 (02.03.04)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/15779

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 00/72119 A2 (Rabin, M.O. & Shasha, D.E.), 30 November, 2000 (30.11.00), Full text; Figs. 1 to 15 & CA 2368861 A & AU 4813700 A & EP 1180252 A2 & CN 1361882 T & JP 2003-500722 A	11-14, 24-36
Y	JP 2001-84137 A (Matsushita Electric Industrial Co., Ltd.), 30 March, 2001 (30.03.01), Par. No. [0089]	7, 17
Y	Par. Nos. [0053] to [0056] (Family: none)	13, 28, 29, 35
A	JP 2002-163578 A (Kabushiki Kaisha Kuredisuto), 07 June, 2002 (07.06.02), Full text; Figs. 1 to 21 (Family: none)	1-36
A	JP 2002-351564 A (NTT Communications Kabushiki Kaisha), 06 December, 2002 (06.12.02), Full text; Figs. 1 to 11 (Family: none)	1-36

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/15779

Box I Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-23 are characterized in that second software and an execution control program are distributed to a user computer, the second software is decoded by using predetermined information and replace it with first software, start information is created according to predetermined information so as to start the second software, and when the execution of the second software is terminated, it is incapacitated.

(Continued to extra sheet)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest ☐ The additional search fees were accompanied by the applicant's protest.
☒ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/15779

Continuation of Box No. II of continuation of first sheet(1)

The inventions of claims 24-36 are characterized in that continuation of execution of application software is allowed or not allowed according to continuation confirmation communication performed with the execution control program at a predetermined timing. Between the group of inventions of claims 1-23 and the group of inventions of claims 24-36, there exists no other common feature which can be considered as a special technical feature within the meaning of PCT Rule 13.2, second sentence. Accordingly, no technical relationship within the meaning of PCT Rule 13 between the different inventions can be seen.

Consequently, claims 1-36 do not satisfy the requirement of unity of invention.

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int. C1' G06F 1/00

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int. C1' G06F 1/00, 12/14, 15/00

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1922-1996年
 日本国公開実用新案公報 1971-2004年
 日本国登録実用新案公報 1994-2004年
 日本国実用新案登録公報 1996-2004年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
Y	J P 2002-229660 A (株式会社東芝) 2002. 08. 16、全文、第1-5図 (ファミリーなし)	1-23
Y	J P 10-133869 A (小川伸一郎) 1998. 05. 22、全文、第1-2図 (ファミリーなし)	1-23
Y	J P 8-6784 A (日本電信電話株式会社) 1996. 01. 12、全文 (特に段落【0053】)、 第1-3図 (ファミリーなし)	1-23

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの
 「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
 「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)
 「O」口頭による開示、使用、展示等に言及する文献
 「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献
 「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
 「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
 「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
 「&」同一パテントファミリー文献

国際調査を完了した日

23. 02. 2004

国際調査報告の発送日

02. 3. 2004

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

林 毅

5B

9193

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		関連する
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	請求の範囲の番号
Y	WO 00/72119 A2 (Rabin, M. O. & Shasha, D. E.)、2000. 11. 30、 全文、第1-15図 & CA 2368861 A & AU 4813700 A & EP 1180252 A2 & CN 1361882 T & JP 2003-500722 A	11-14、24-36
Y	JP 2001-84137 A (松下電器産業株式会社) 2001. 03. 30 段落【0089】	7、17
Y	段落【0053】-【0056】 (ファミリーなし)	13、28、29、35
A	JP 2002-163578 A (株式会社クレディスト) 2002. 06. 07、全文、第1-21図 (ファミリーなし)	1-36
A	JP 2002-351564 A (エヌ・ティ・ティ・コミュニケーションズ株式会社) 2002. 12. 06、全文、第1-11図 (ファミリーなし)	1-36

第 I 欄 請求の範囲の一部の調査ができないときの意見 (第 1 ページの 2 の続き)

法第 8 条第 3 項 (PCT 17 条 (2) (a)) の規定により、この国際調査報告は次の理由により請求の範囲の一部について作成しなかった。

1. ☐ 請求の範囲 _____ は、この国際調査機関が調査をすることを要しない対象に係るものである。
つまり、
2. ☐ 請求の範囲 _____ は、有意義な国際調査をすることができる程度まで所定の要件を満たしていない国際出願の部分に係るものである。つまり、
3. ☐ 請求の範囲 _____ は、従属請求の範囲であって PCT 規則 6.4(a) の第 2 文及び第 3 文の規定に従って記載されていない。

第 II 欄 発明の単一性が欠如しているときの意見 (第 1 ページの 3 の続き)

次に述べるようにこの国際出願に二以上の発明があるところの国際調査機関は認めた。

請求の範囲 1-23 に係る発明は、第 2 のソフトウェアと実行制御プログラムをユーザコンピュータに配信し、所定の情報を用いて第 2 のソフトウェアをデコードして第 1 のソフトウェアに置き換え、所定の情報に基づいて起動情報を生成して第 2 のソフトウェアを起動し、第 2 のソフトウェアの実行が終了するとこれを無効化することを特徴とし、請求の範囲 24-36 に係る発明は、所定の時期に実行制御プログラムとの間で行われる継続確認通信に基づいてアプリケーションソフトウェアの実行継続を許可するか否かを管理することを特徴とするから、請求の範囲 1-23 に係る発明と、請求の範囲 24-36 に係る発明との間には、PCT 規則 13.2 の第 2 文の意味において、特別な技術的特徴と考えられる他の共通事項は存在しないので、これらの発明の間に PCT 規則 13 の意味における技術的な関連を見いだすことはできない。

よって、請求の範囲 1-36 は、発明の単一性の要件を満たしていない。

1. ☒ 出願人が必要な追加調査手数料をすべて期間内に納付したので、この国際調査報告は、すべての調査可能な請求の範囲について作成した。
2. ☐ 追加調査手数料を要求するまでもなく、すべての調査可能な請求の範囲について調査することができたので、追加調査手数料の納付を求めなかった。
3. ☐ 出願人が必要な追加調査手数料を一部のみしか期間内に納付しなかったため、この国際調査報告は、手数料の納付のあった次の請求の範囲のみについて作成した。
4. ☐ 出願人が必要な追加調査手数料を期間内に納付しなかったため、この国際調査報告は、請求の範囲の最初に記載されている発明に係る次の請求の範囲について作成した。

追加調査手数料の異議の申立てに関する注意

- ☐ 追加調査手数料の納付と共に出願人から異議申立てがあった。
☒ 追加調査手数料の納付と共に出願人から異議申立てがなかった。